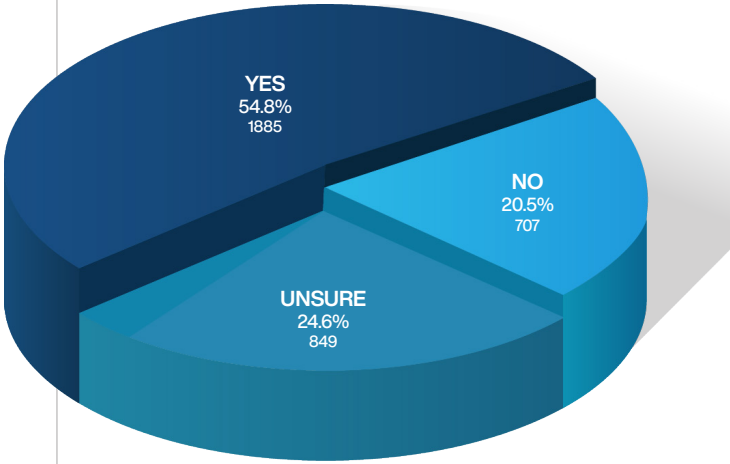
STATE OF CYBER 2024

SECURITY IN DEPTH

Table of Contents



Legend:

Throughout this document, you will see statistical information in the form of various graphs. The percentage indicates the percentage of all surveyed, while the number underneath indicates the total number of respondents for that answer.

YES 54.8% 1885	=	ANSWER PERCENTAGE No. OF RESPONDENTS

Table of Contents

Executive Summary

In an era marked by a rapidly evolving cyber threat landscape, the situation in Australia, as detailed in Security in Depth's "State of Cyber Security" report, presents a stark illustration of the escalating challenges faced by businesses, particularly small to medium-sized enterprises (SMBs).

This report sheds light on the severity and frequency of cyber incidents that far exceed the commonly reported statistics, underscoring a pervasive vulnerability across the nation.

The "State of Cyber Security" report reveals a concerning trend of increasing cyber incidents in Australia. In 2023 alone, there were **11,784** reports of organisations being hacked, a significant escalation from previous years. Phishing attacks, a barometer of cyber threats, saw a dramatic rise to **99,736** successful incidents, up from **74,574** in 2022. Identity thefts also saw an upward trajectory with **18,592** Australians falling victim over the last 12 months, increasing from **16,212** in 2022. These figures highlight not only the frequency but also the sophistication of cyber attacks targeting Australian entities.

The financial implications of these incidents are staggering. In 2023, credit card theft reached a record high with **4.597 million** instances reported across Australia. The total economic loss attributed to cybercrime soared to an alarming **3.2 billion dollars**, with only a fraction, **about 47 million dollars**, being recovered. This data underscores the profound financial impact cybercrime has on the Australian economy and individual businesses, particularly SMBs.

The report's findings underscore the vulnerability of SMBs, which form the backbone of the Australian economy. These businesses are particularly susceptible to cyber threats due to a general lack of preparedness. Key areas such as governance, understanding and

adoption of security frameworks, and reliance on IT teams are identified as critical gaps. These gaps are exacerbated by inadequate and irregular training, leaving employees vulnerable to sophisticated cyber scams such as phishing.

11,784 reports of organisations being hacked

99,736 successful phishing attacks

18,592 reports of identity theft

Further compounding these challenges is the lack of comprehensive incident response plans and effective detection of attacks, leaving businesses exposed to significant risks. The report also highlights that many systems and networks remain unpatched, making them easy targets for threat actors who often exploit vulnerabilities soon after their discovery.

The insights provided in Security in Depth's "State of Cyber Security" report serve as a potent reminder of the urgent need for Australian businesses to address their cybersecurity challenges. This situation calls for a strategic overhaul in cybersecurity practices, emphasizing the adoption of comprehensive and standardized security frameworks, investment in skilled cybersecurity personnel, and fostering a culture of continuous improvement and vigilance against the evolving cyber threat landscape.

In conclusion, the state of cyber security in Australia, as detailed in Security in Depth's report, is at a critical juncture. The scale and sophistication of cyber threats demand a concerted and proactive response, especially from SMBs, which are most vulnerable yet integral to the national economy. The time to act is now, to safeguard not only individual businesses but also the broader economic and national security framework of Australia.

Methodology Overview

1. Survey Design and Distribution

The cornerstone of our research methodology is a comprehensive survey, tailored to meticulously capture a broad spectrum of data on cybersecurity practices within Australian organisations.

Key features of the survey include:

- **Tailored Questions:** Customised to cater to the unique cybersecurity frameworks of diverse organisations, ensuring relevance and comprehensiveness.
- **Inclusive Content:** A broad coverage of aspects including current security measures, incident response protocols, employee cybersecurity awareness, and resource allocation to provide a holistic understanding.
- **Digital Accessibility:** Utilisation of digital platforms to enhance accessibility and participation, ensuring a representative sample.
- **Confidentiality Assurance:** Implementation of measures to guarantee respondent anonymity and data privacy, encouraging candid and accurate responses.

2. Interview Process

Structured interviews complement the survey phase, aimed at obtaining deeper insights from key personnel within organisations.

This phase focuses on:

- **Garnering Depth:** Exploring the intricacies of cybersecurity challenges and practices beyond what survey data can reveal.
- **Real-World Perspectives:** Gaining insights into the practical implementation of cybersecurity measures and the challenges encountered.
- **Facilitating Dialogue:** Encouraging open discussion on experiences, concerns, and recommendations for cybersecurity enhancement.
- **Building Partnerships:** Developing collaborative relationships with participants for ongoing cybersecurity research and improvement.

3. Data Analysis

A rigorous analysis of the collected data employs both quantitative and qualitative methods to ensure a comprehensive understanding of the cybersecurity posture of Australian organisations.

This includes:

- **Quantitative Examination:** Statistical analysis to identify trends, patterns, and correlations across diverse organisations.
- **Qualitative Insights:** Thematic analysis of interview responses to understand the narratives and perspectives behind the data.
- **Cross-Referencing:** Integration of insights from both surveys and interviews for a nuanced understanding of the cybersecurity landscape.
- **Advanced Analytical Tools:** Utilisation of sophisticated software and methodologies to enhance the accuracy and depth of findings.

4. Benchmarking Against International Standards

A critical aspect of our methodology is the strategic benchmarking of organisational practices against the NIST cybersecurity framework and ISO27001 standards.

This process includes:

- **Comparative Analysis:** Evaluating how organisational practices align with or diverge from these recognized benchmarks.
- **Gap Identification:** Highlighting areas for potential improvement and alignment with global standards.
- **Customised Recommendations:** Developing actionable, tailored strategies for each organisation based on benchmark analysis.
- **Global Best Practices Advocacy:** Emphasising the importance of adhering to internationally recognised cybersecurity frameworks for enhanced resilience.

Enhanced Methodology Components

Our methodology is further distinguished by its emphasis on enhanced confidentiality, ethical considerations, and continuous ethical training. Rigorous adherence to privacy laws, informed consent, transparency, and cultural sensitivity ensures the integrity and ethical conduct of the research, fostering trust and cooperation from participants.

Conclusion

This comprehensive research methodology is designed to provide an in-depth analysis of the cybersecurity landscape across Australian organisations. By integrating tailored surveys, in-depth interviews, rigorous data analysis, and benchmarking against international standards, while upholding the highest ethical standards, this study aims to contribute significantly to the understanding of cybersecurity readiness and resilience among Australian organisations. The findings are expected to inform strategic decision-making, policy formulation, and the implementation of effective cybersecurity measures, aligning with global best practices for a more secure digital environment.

Financial Impact of a Cyber Incident on Business

In 2023, the cybersecurity landscape revealed significant financial impacts on businesses of different sizes, as highlighted by Security in Depth research. This comprehensive analysis underscores the varying effects of cybercrime on enterprises based on their scale.

Here's a detailed overview:

1. **Small Businesses:**
   Small enterprises faced an average loss of $52,213 per cybercrime incident. This figure underscores the vulnerability of smaller businesses, which often lack robust cybersecurity defenses.

2. **Medium Businesses:**
   Medium-sized businesses, classified by the Australian Bureau of Statistics as having between 20 and 199 employees, encountered the highest average loss, amounting to $116,697. This substantial loss can be ascribed to several factors:

   - **Lower Implementation of Cybersecurity Measures:**
     Compared to larger corporations, medium-sized enterprises are generally less likely to implement comprehensive cybersecurity measures. These measures are crucial in reducing the likelihood and severity of cyber incidents.
   - **Greater Propensity to Report Cybercrime:**
     Medium-sized organisations might be more inclined to report cybercrimes due to their limited in-house or commercial incident response capabilities, unlike larger organisations.

3. **Large Businesses:**
   Larger corporations reported an average loss of $82,148 per cybercrime incident. Although they incur significant losses, larger businesses typically have more advanced cybersecurity protocols in place, potentially contributing to their relatively lower average loss compared to medium-sized enterprises.

Small Business losses:

$52,213
per incident

Medium Business losses:

$116,697
per incident

Large Business losses:

$882,148
per incident

Cost Analysis of Cyber Incidents in Small Organisations

The following cost breakdown is derived from a comprehensive analysis conducted by Security in Depth, encompassing 22 small organisations that encountered cyber incidents during the calendar year 2023. These organisations typically maintained an average staff size of 6 full-time employees, supporting 925 active customers and 390 non-active customers. Notably, none of the organisations had Cyber Insurance coverage.

1. **Legal Fees:**
   Legal consultation and representation: $10,000
   Total Legal Fees: $10,000

2. **Digital Forensics:**
   Forensic investigation services: $8,000
   Data breach analysis: $5,000
   Total Digital Forensics: $13,000

3. **Communication Requirements:**
   Notification letters to customers: $2,000
   Public relations and crisis communication management: $5,000
   Total Communication Requirements: $7,000

4. **Additional Technical Requirements:**
   Technology: Upgrades and patches - $5,000
   Time: External IT consultant for 5 days - $5,000
   Total Additional Technical Requirements: $10,000

5. **Staff Training and Awareness:**
   Cybersecurity awareness training: $450
   Total Staff Training and Awareness: $450

6. **Customer Remediation and Support:**
   Customer support for inquiries and concerns: $2,000
   Credit monitoring services for affected customers: $3,000
   Total Customer Remediation and Support: $5,000

7. **Consultation and Incident Response Management:**
   Hiring external incident response consultants: $5,000
   Coordination and management of incident response efforts: $3,000
   Total Consultation and Incident Response Management: $8,000

Additional Observations:

- **Loss of Work Time for Staff Members:** The combined loss of work time for staff members across all organisations totalled 11.5 days. this resulted in an additional cost of approximately $39,692.31 in loss productivity (this does not include revenue generation lost).
- **Potential Loss of Business and Productivity:** The loss of 4 days of this work translated to a potential loss of business and productivity amounting to approximately $13,846.15

In conclusion, the comprehensive cost analysis reveals the significant financial impact of cyber incidents on small organisations, underscoring the importance of proactive cybersecurity measures and incident response strategies to mitigate risks and minimise financial losses.

Cost Analysis of Cyber Incidents in Small Organisations (cont.)

The cost analysis conducted by Security in Depth on the repercussions of cyber incidents in small organisations during 2023 sheds light on the substantial financial and operational challenges these entities face.

With a focus on 22 small organisations that support a considerable customer base yet lack Cyber Insurance, the findings reveal significant expenses across various domains including legal fees, digital forensics, communication, technical upgrades, staff training, customer remediation, and incident response management. Notably, legal consultation and digital forensic investigations emerged as major cost centres, emphasising the critical need for specialised services in the aftermath of cyber incidents.

Further compounding the issue is recent research indicating that only 12% of the 2.5 million Australian businesses have cyber insurance. This stark figure suggests a widespread vulnerability, with the majority of businesses potentially facing even greater financial risks in the absence of insurance coverage. The direct costs detailed in the report, combined with the indirect costs such as lost productivity and potential loss of business, paint a concerning picture for uninsured businesses. These findings serve not as a cause for alarm but as a factual exposition of the current state of cybersecurity readiness among Australian businesses. The low uptake of cyber insurance underscores a critical gap in the cybersecurity posture of these entities, emphasising the need for greater awareness and adoption of cyber insurance as part of a holistic risk management strategy.

The data presented by Security in Depth, along with the insights on cyber insurance uptake, highlight the multifaceted nature of cyber risk management. They underscore the importance of not only investing in preventive measures and specialised incident response services but also in considering cyber insurance as a key component of a comprehensive cybersecurity strategy. This approach is crucial for mitigating the financial impacts of cyber incidents, ensuring operational resilience, and safeguarding customer trust in an increasingly digital business landscape.


75%
45%
20%
STATE OF CYBER
%include "win32n.inc"
extern MessageBoxA
import MessageBoxA user32.dll

The State of Cyber Security

Overall Increase in Cyber Incidents:

The year saw a 37% increase in cyber incidents, indicating a rise in more advanced and focused attacks.

- **Financial Impact on Small Businesses:**
  Small enterprises faced an average loss of $52,213 per cybercrime incident.
  These businesses often lack robust cybersecurity defenses, making them particularly susceptible to devastating financial impacts.
- **Medium Businesses Bear the Brunt:**
  Medium-sized businesses experienced the highest average loss at $116,697 per incident.
  This is attributed to a lower implementation of cybersecurity measures compared to larger corporations and a greater propensity to report cybercrimes.
- **Large Businesses' Losses:**
  Larger corporations reported an average loss of $82,148 per cybercrime incident. While significant, these losses are relatively lower compared to medium-sized enterprises, likely due to more advanced cybersecurity protocols in larger organisations.
- **Phishing and Identity Thefts:**
  The year witnessed 99,736 successful phishing attacks, up from 74,574 in 2022, and 18,592 Australians had their identities stolen, an increase from 16,212 in the previous year.
- **Credit Card Thefts and Economic Losses:**
  Credit card thefts hit a record high with 4.597 million instances, and the total economic loss due to cybercrime soared to 3.2 billion dollars, with only 47 million recovered.
- **Cybercrime Reports by Business Size:**
  11,784 reports of organisations being hacked highlight the widespread nature of cyber threats across all business sizes.
- **Disproportionate Impact Across States:**
  Queensland and Victoria reported higher rates of cybercrime relative to their populations, with the Northern Territory and Western Australia experiencing the highest average reported losses.

Small Business:

$52,213 per incident.

Medium Business:

$116,697 per incident.

Large Businesses':

$882,148 per incident.

Phishing and Identity Thefts:

99,736 successful phishing attacks
18,592 Australians had their identities stolen

Credit Card Thefts and Economic Losses:

4.597 million instances totalling $3.2 billion dollars
(with only $47 million recovered).

11,784 organisations hacked

Cyber Security Incidents by Sector

The distribution of cyber incidents across various sectors in Australia, as detailed in Security in Depth's "State of Cyber Security" report, paints a revealing picture of the current cyber threat landscape.

The percentages reflect the proportion of cyber incidents experienced by different sectors, highlighting the vulnerability and targeted nature of cyber attacks in specific industries.

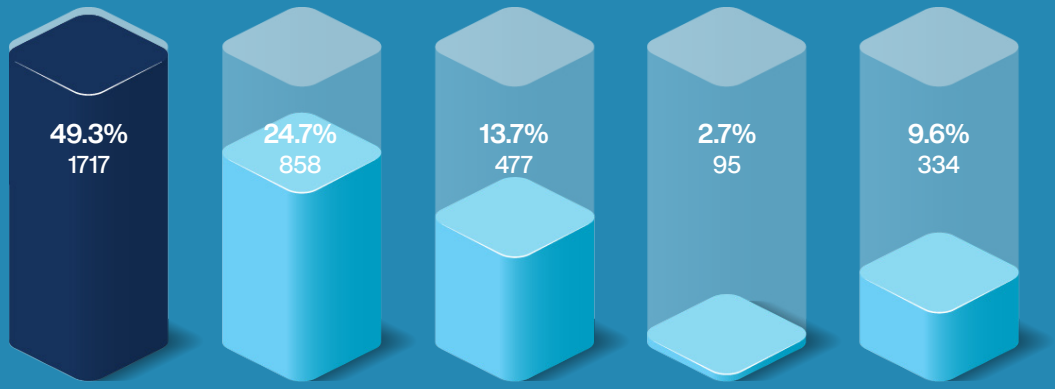
- **Government - Commonwealth (23.10%):**
  This sector's high percentage suggests that cybercriminals often target national government entities, likely due to the valuable and sensitive nature of the information they hold. The high figure also reflects the increasing geopolitical motivations behind cyber attacks.
- **Professional, Scientific and Technical Services (12.80%):**
  The significant targeting of this sector indicates that cybercriminals are attracted to the intellectual property and proprietary data these businesses often manage. This sector's reliance on digital technology makes it a lucrative target for cyber attacks.
- **Financial and Insurance Services (11.20%):**
  As a sector that deals with vast amounts of financial data and transactions, it's not surprising to see it heavily targeted. The financial incentives for cybercriminals are considerable here, making it a consistent focus for attacks.
- **Government - State/Territory/Local (9.62%):**
  Similar to the Commonwealth Government, these levels of government are attractive targets due to the sensitive citizen data and critical public services they oversee.
- **Health Care and Social Assistance (9.61%):**
  The close percentage to State and Territory Governments underlines the critical nature of this sector, especially with its wealth of personal health data. The pandemic and increased digitalization of health records may have heightened its vulnerability.
- **Information Media and Telecommunications (8.10%):**
  This industry, being at the forefront of information dissemination and digital infrastructure, is a natural target for cyber attacks aimed at disrupting communications or stealing sensitive information.
- **Education and Training (6.57%):**
  Educational institutions store vast amounts of personal data and research information, making them attractive targets for cybercriminals, especially for ransomware and data theft.
- **Construction (4.00%) and Manufacturing (4.00%):**
  These sectors, while lower on the list, still face significant risks. The impact on these industries can be substantial, disrupting operations and supply chains.
- **Electricity, Gas, Water, and Waste Services (3.00%):**
  Critical infrastructure sectors, though lower in percentage, face high risks of cyber attacks aimed at causing widespread disruption and damage.

This distribution of cyber incidents by sector underscores the need for a targeted approach to cybersecurity across different industries. It reflects the diverse motivations of cybercriminals - from financial gain in the financial sector to espionage in government entities and intellectual property theft in technical services. Each sector requires tailored cybersecurity strategies that consider their specific risks and vulnerabilities.


GOVERNANCE

Question:

What cyber risk are you most concerned about when it comes to your personal cybersecurity?



The survey shows that the predominant cyber risk concern for individuals regarding their personal cybersecurity is identity theft and cyber extortion, such as ransomware, at 49.32%. This is followed by concerns about losing money or valued data due to a cyberattack, which accounts for 24.66% of the responses.

Concerns about critical infrastructure breakdown due to cyberattacks are next at 13.70%, while smaller percentages are worried about geopolitical instability and cyberwar (2.74%) and blackmail from compromised personal data (9.59%). Notably, no respondents reported concerns over falsified or stolen medical data.

This distribution of concerns correlates with the increasing frequency of ransomware attacks and the high-profile nature of such incidents, which often result in significant personal and financial losses. The fear of losing personal wealth or data reflects a growing awareness of the direct impact that cyberattacks can have on individuals.

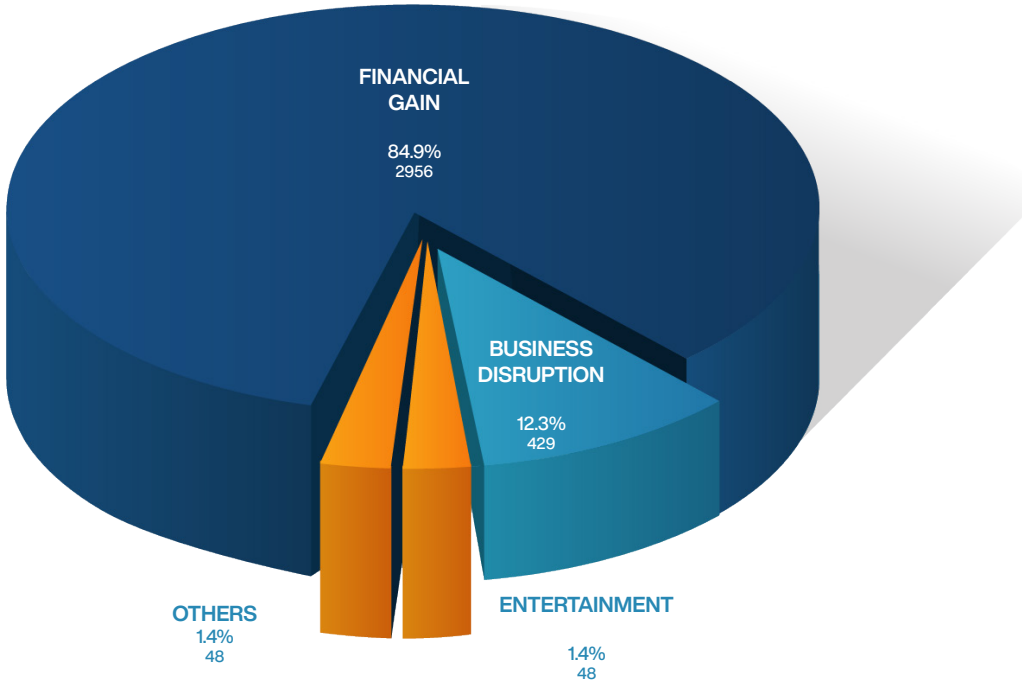
However, the lack of concern for falsified or stolen medical data is surprising, given the sensitivity of health information and the potential for its misuse. This could suggest a lack of awareness about this type of threat, or it could be that respondents prioritize other risks higher based on their perception or experience.

Considering the previous survey data, which indicated a need for better risk management strategies and more consistent cybersecurity training, the expressed concerns highlight the need for individualized approaches to personal cybersecurity. While organisations are responsible for safeguarding their systems and data, individuals also need to be aware of the risks and take steps to protect their personal information, especially given the prevalence of identity theft and financial fraud.

In summary, the survey results emphasize the importance of comprehensive cybersecurity strategies that address not only organisational needs but also the personal concerns of individuals within these organisations. This includes regular awareness training that covers a broad range of cyber risks, including those that may not yet be widely recognized, such as threats to medical data.

Question:

What do you believe is the primary focus of cyber attacks?



The 2023 State of Cyber Security Survey indicates an overwhelming consensus among respondents that financial gain is the primary motivator behind cyber attacks, with 84.93% aligning with this perspective.

This is followed by a smaller fraction, 12.33%, who consider business disruption as the main focus. Notably, reputational damage and revenge are not seen as primary drivers, as indicated by 0% of respondents for each category. Entertainment and other unspecified reasons are considered the main focus by 1.37% of respondents respectively.

This data reflects a recognition that cyber attacks are largely profit-driven, aligning with global trends where ransomware and data breaches for financial extortion are rampant. The lack of concern for reputational damage or revenge as motivators may indicate that respondents view cyber attacks more as a professional criminal enterprise rather than actions driven by personal vendettas or for the purpose of inflicting reputational harm.

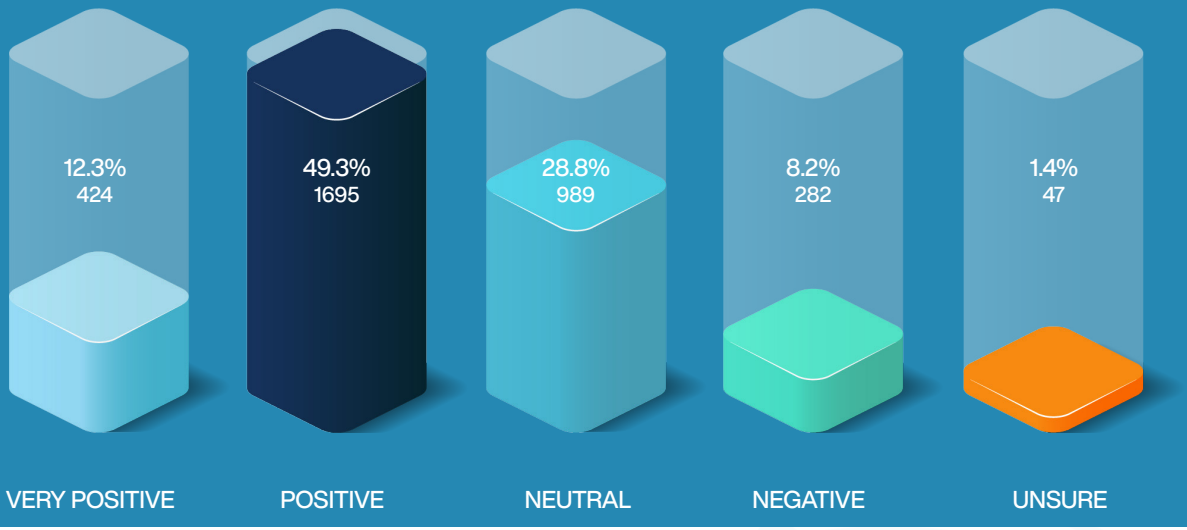
Considering the perceived lack of focus on reputational damage, it is essential to acknowledge that while it may not be the primary goal, it is often a consequential outcome of cyber attacks. Therefore, organisations should not underestimate the reputational impact when strategizing their cybersecurity measures.

The recognition of financial gain as the primary objective underscores the necessity for robust financial and data protection systems. It also stresses the importance of regular security training focused on recognizing and mitigating attacks that could lead to financial loss, such as phishing and social engineering tactics.

In summary, the survey results highlight the importance of understanding the motivations behind cyber attacks to better tailor cybersecurity defenses. It is clear that organisations need to prioritize the protection of financial assets and sensitive data, as these are the most lucrative targets for cybercriminals.

Question:

How do you feel about your organisation's ability to be cyber resilient?



The data reveals that respondents have varied levels of confidence in their organisation's cyber resilience.

A combined total of 61.65% feel positive or very positive about their ability to withstand cyber threats, which is indicative of a strong confidence in their current cybersecurity measures and strategies. However, a noteworthy 28.77% of respondents have a neutral stance, while 8.22% hold a negative view, and 1.37% are unsure about their organisation's cyber resilience.

The optimistic view of over half of the respondents is encouraging, as it suggests that a significant number of organisations are taking steps to bolster their cyber defenses and may feel prepared to face potential cyber threats. This could be reflective of effective risk management strategies, regular cybersecurity training, and other proactive measures being implemented within these organisations.

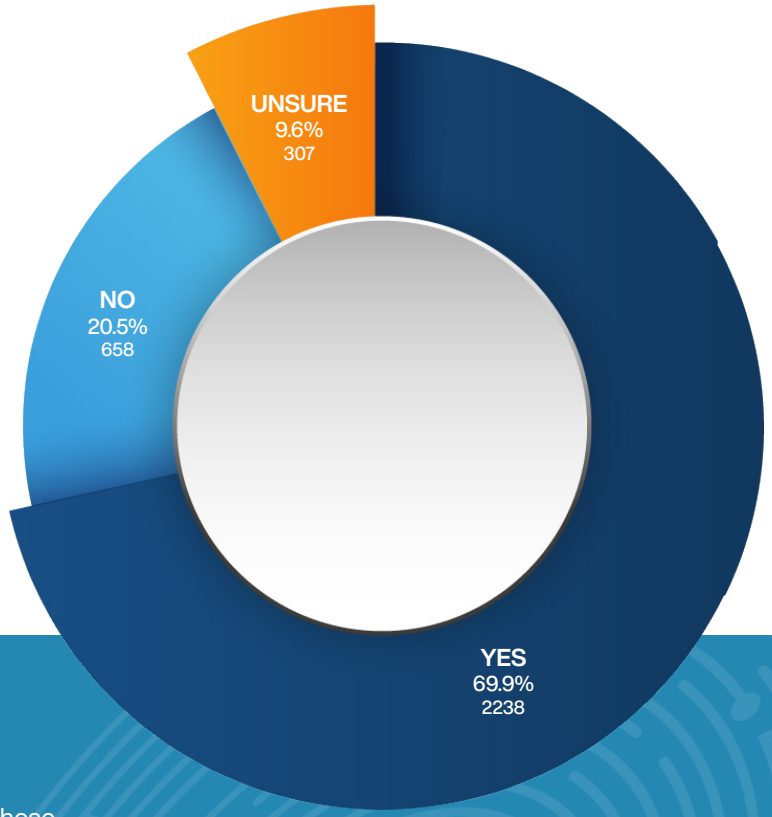
The neutral and negative perceptions, along with those who are unsure, highlight that there is still a considerable segment of the business community that either recognizes the need for improvement in their cybersecurity posture or may lack the necessary resources or knowledge to effectively evaluate their state of preparedness.

The data underscores the importance of continuous improvement in cybersecurity practices, considering the evolving nature of cyber threats. Organisations should strive to move from neutral or negative sentiments towards a more positive outlook by investing in robust cybersecurity frameworks, regular risk assessments, and employee training programs.

In conclusion, while many organisations are confident in their cyber resilience, the survey data points to the need for ongoing efforts to maintain and enhance cybersecurity measures to ensure that this confidence is well-founded and that all organisations can work towards achieving a very positive state of cyber resilience.

Question:

Do you currently have risk management strategies for cyber security in your business?



According to the 2023 State of Cyber Security Survey, a majority of respondents, 69.86%, report having risk management strategies for cybersecurity in place.

This suggests a general recognition of the importance of proactive measures to manage and mitigate cyber threats. However, there is still a significant portion, 20.55%, that does not have such strategies, and 9.59% are unsure of their stance on risk management in cybersecurity.

The presence of risk management strategies is a positive indicator that many businesses are taking steps to address cybersecurity proactively. It is essential, given the interconnected nature of digital business operations and the increasing sophistication of cyber threats.

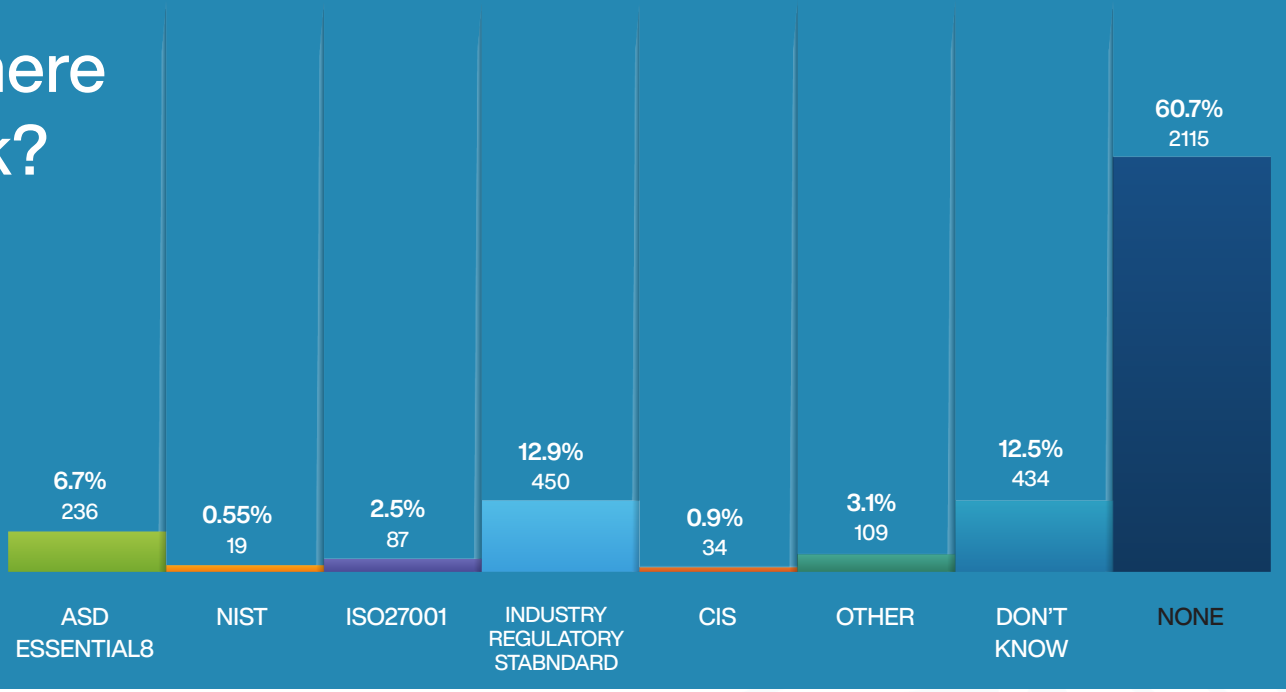
However, the lack of risk management strategies in over a fifth of businesses leaves them vulnerable to the wide-reaching consequences of cyber incidents. This vulnerability is underscored by the previous data points, including the high percentage of organisations not monitoring for reused passwords and the considerable number not engaging in third-party cybersecurity audits or having cyber insurance.

The uncertainty reported by some organisations about their cybersecurity risk management strategies suggests a need for better communication and education within these businesses. It highlights the necessity for clear, actionable plans that are understood and implemented across the organisation.

Overall, while it's encouraging that many organisations are implementing risk management strategies for cybersecurity, there's still a need to close the gap for those without such strategies and to ensure that the strategies in place are effective, regularly updated, and part of a holistic approach to cybersecurity.

Question:

Does your organisation adhere to an IT Security framework?



The diverse adoption of IT security frameworks among surveyed Australian organisations highlights the need for greater awareness, education, and resources to support the implementation of comprehensive cybersecurity practices.

As cyber threats continue to evolve, it is crucial for organisations to adopt structured and standardized IT security frameworks to enhance their cybersecurity posture and contribute to a more secure and resilient business landscape.

1. **Predominance of non-adherence:**
The most striking observation from the survey is that a majority (60.71%) of the organisations do not adhere to any IT security framework, potentially leaving them more vulnerable to cyber threats due to a lack of structured and standardized cybersecurity practices.

2. **Industry Regulatory Standards:**
The relatively high percentage (12.92%) of organisations adhering to industry regulatory standards suggests that, for many businesses, compliance with specific regulations may be the primary driver for implementing cybersecurity measures, rather than adopting a more comprehensive security framework.

3. **Limited adoption of widely recognized frameworks:**
The low adoption rates of internationally recognized IT security frameworks, such as NIST (0.55%), ISO27001 (2.50%), and CIS (0.98%), may indicate a lack of awareness or resources to implement these frameworks effectively.

4. **Uncertainty around adherence:**
The fact that 12.46% of respondents reported not knowing whether their organisation adheres to an IT security framework suggests a potential communication gap within these organisations, which may hinder their ability to effectively manage cybersecurity risks.

Question:

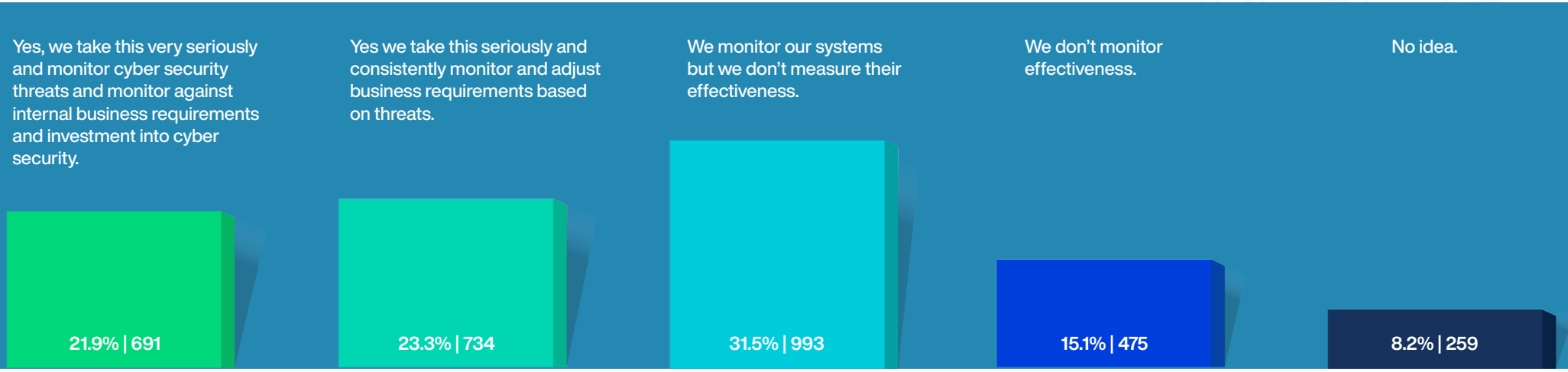
Does your organisation measure the effectiveness of cybersecurity implementations and actions across your business?

From the 2023 State of Cyber Security Survey, it is evident that organisations vary in their approach to measuring the effectiveness of cybersecurity implementations. A proactive segment (21.92%) seriously monitors cybersecurity threats in alignment with internal business requirements and investments, while a slightly larger group (23.29%) not only monitors but also actively adjusts their business requirements based on the evolving threat landscape.

However, a significant portion of respondents (31.51%) monitor their systems without measuring effectiveness, which could indicate a lack of comprehensive cybersecurity strategy or a gap in their ability to evaluate their defensive measures. Furthermore, 15.07% of organisations do not monitor the effectiveness of their cybersecurity at all, suggesting a notable area of vulnerability. The 8.22% who have no idea about their monitoring status highlight a concerning lack of awareness or engagement with cybersecurity practices.

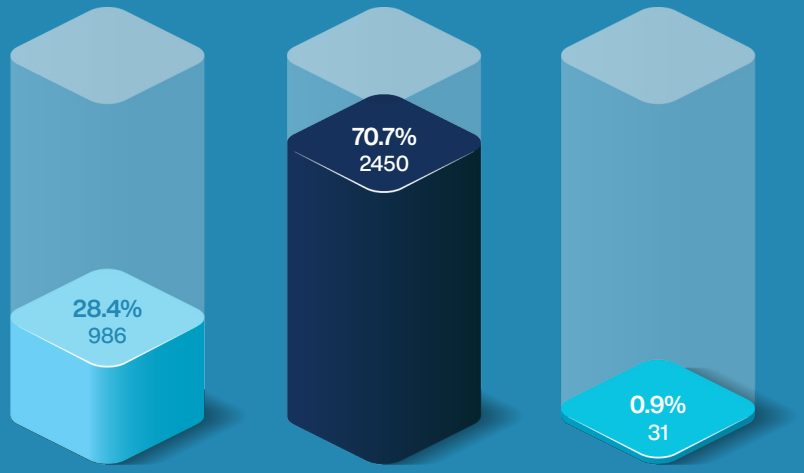
When considering the earlier survey responses, which reflect various levels of cybersecurity maturity and preparedness, these figures suggest that while some organisations are making concerted efforts to ensure their cybersecurity measures are effective, there is still a substantial number of businesses that need to develop or improve their monitoring and evaluation processes.

The data underscores the importance of not only implementing cybersecurity solutions but also continuously assessing and refining these measures to ensure they remain effective against an ever-changing threat landscape. It also points to the necessity for better education and communication regarding the importance of monitoring and evaluation in the field of cybersecurity.



Question:

Have you ever had an independent party conduct an audit of your computer systems and processes?



The data presented reveals that only 28.44% of organisations have engaged an independent party to audit their computer systems and processes.

While this figure is notably higher than the percentage of organisations that have fully tested their cyber incident response plan with an external organisation (1.84%), it still indicates that a significant majority, 70.67%, have not conducted such an audit. Additionally, a small fraction remains unsure about whether they have undergone an independent audit.

The implications of these statistics are multifaceted. First, they suggest that while there is some acknowledgment of the value of independent oversight, the majority of organisations may not fully recognize the benefits of external audits. These audits are crucial as they provide an objective assessment of an organisation's cybersecurity posture, identifying vulnerabilities that internal teams may miss due to familiarity biases or resource constraints.

Secondly, the data may reflect a disparity in resource allocation toward cybersecurity initiatives. Smaller organisations might lack the financial or operational capacity to engage in external audits, whereas larger organisations, despite having more resources, may not prioritize them. This could be due to a variety of reasons, including a false sense of security, a lack of understanding of the current threat landscape, or the perceived adequacy of internal controls.

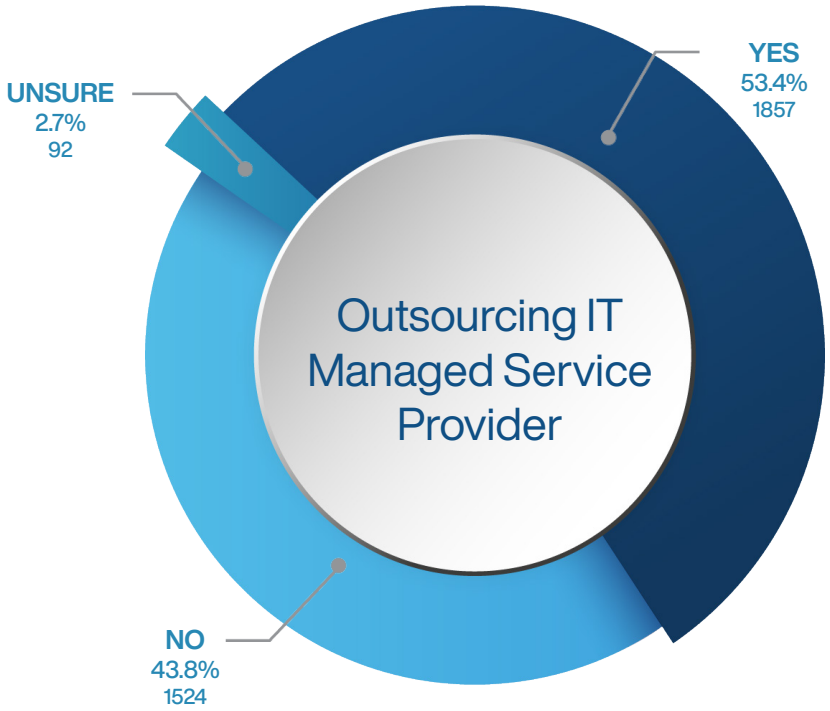
The relatively small number of organisations that are unsure whether they have conducted such an audit further underscores a potential lack of communication and governance within these organisations concerning cybersecurity matters. It is concerning that any organisation would be uncertain about such a critical component of cybersecurity management.

Considering the low numbers of organisations with a written incident response plan and those that have fully tested their response plan, it is not entirely surprising to see a similar trend in the auditing practices. However, this consistency points to a broader trend of cybersecurity being undervalued or misunderstood as a critical business function.

The need for industry-wide education on the risks of inadequate cybersecurity practices is apparent. There is a pressing requirement for clear guidelines and standards that organisations can realistically adopt and implement. Furthermore, there is an opportunity for cybersecurity service providers to address this gap by offering scalable solutions for businesses of all sizes.

Question:

Do you outsource your IT to a Managed Service Provider



The survey indicates that a majority of the respondents, 53.42%, outsource their IT to a managed service provider. This suggests a significant reliance on external expertise to manage IT needs, which could include cybersecurity management and support.

Conversely, 43.84% retain their IT operations in-house, while a small portion, 2.74%, are unsure about their IT management structure.

The trend towards outsourcing IT to specialized providers can be seen as a strategic move, particularly for small to medium-sized businesses that may not have the resources to maintain a full-fledged IT department. Managed service providers often bring a level of expertise and efficiency that can be cost-prohibitive for individual organisations to develop internally. They can also offer scalability and access to advanced technologies and methodologies, including cybersecurity services, which are crucial in the current digital landscape.

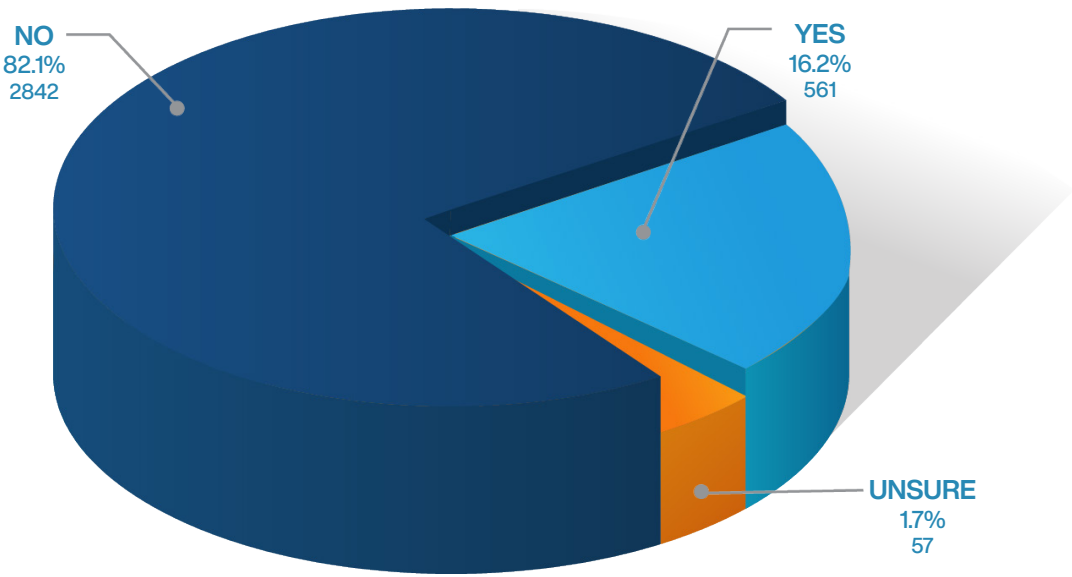
However, this reliance on external IT services also raises important considerations regarding the oversight and governance of cybersecurity practices. Organisations must ensure that their managed service providers have robust cybersecurity measures and that there is clear communication regarding the division of responsibilities for protecting against and responding to cyber incidents.

For the segment of organisations not outsourcing their IT, it is essential to recognize the importance of developing strong internal capabilities, particularly in cybersecurity, which is increasingly becoming a non-negotiable aspect of doing business in the digital age. The small percentage of respondents unsure about their IT management approach points to a potential area for improvement in terms of strategic IT planning and policy development.

The survey data underscores the diverse approaches to IT management and the prominent role of managed service providers in the contemporary cybersecurity ecosystem. Regardless of the approach taken, the data highlights the universal importance of prioritizing cybersecurity within the IT management strategy, whether it is outsourced or managed internally.

Question:

Have you seen or reviewed the cyber security capabilities of your IT provider?



The data presents a concerning picture: only 16.21% of respondents have seen or reviewed the cybersecurity capabilities of their IT provider. This leaves a vast majority, 82.14%, who have not, with a small percentage, 1.65%, unsure about whether they have undertaken such a review.

This finding is particularly striking in the context of the earlier statistic that a majority of organisations outsource their IT to managed service providers. The lack of oversight revealed by these numbers suggests a disconnect between the reliance on external IT services and the due diligence conducted by organisations on the cybersecurity prowess of these providers.

The importance of vetting an IT provider's cybersecurity capabilities cannot be overstated. Given the increasing sophistication of cyber threats and the critical role of IT service providers in managing and protecting organisational data, it is imperative for organisations to actively engage in assessing the security measures implemented by their providers.

The low percentage of organisations that have reviewed their IT provider's cybersecurity capabilities could indicate a lack of awareness of the potential risks involved or a gap in the cybersecurity governance processes within these organisations. It may also reflect an over-reliance on the perceived expertise of IT providers without sufficient verification.

For the organisations that have not conducted such a review, there is an urgent need to establish processes for regular and thorough evaluations of their IT providers' cybersecurity measures. This should be an integral part of the contractual relationship with the provider and include clear communication about expectations, responsibilities, and the right to audit.

The survey data highlights a critical oversight in the cybersecurity practices of a significant number of organisations. It underscores the necessity for a proactive and informed approach to managing third-party IT services, especially in areas as crucial as cybersecurity. Organisations must take steps to ensure that their IT providers are not only capable of delivering services but are also equipped to protect against cyber threats, thereby safeguarding both their own and their clients' data.

Question:

How does your practice gain assurance that project delivery partners and other third-party suppliers are compliant with your security policies?

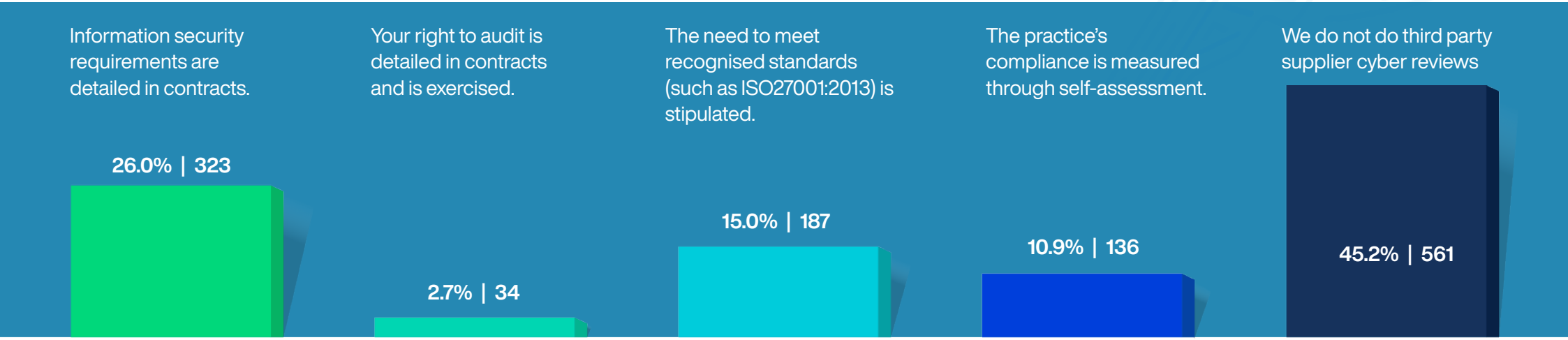
The survey unveils a critical perspective on how organisations assure compliance with security policies among project delivery partners and third-party suppliers. A mere 9.33% of respondents have information security requirements detailed in contracts, and only 7.57% have contractual audit rights that are actively exercised. Slightly more, 7.54%, require adherence to recognized standards such as ISO27001:2013. Interestingly, 14.50% rely on self-assessment measures for compliance. However, the majority, 61.05%, admit to not conducting cyber reviews of third-party suppliers at all.

This data paints a concerning picture of the cybersecurity oversight landscape. The low percentages of organisations that have taken proactive contractual steps or engaged in audit practices suggest a broader trend of insufficient diligence regarding third-party cybersecurity risks. The reliance on self-assessment for compliance measurement, while useful, may not provide the rigorous validation needed to ensure that external parties' security practices align with an organisation's standards.

The most startling revelation, however, is that the significant majority do not conduct third-party supplier cyber reviews. This oversight represents a substantial gap in cybersecurity defenses, given that third-party suppliers can be a common vector for security breaches. In an interconnected digital ecosystem, the security posture of third-party partners is as crucial as that of the contracting organisation itself.

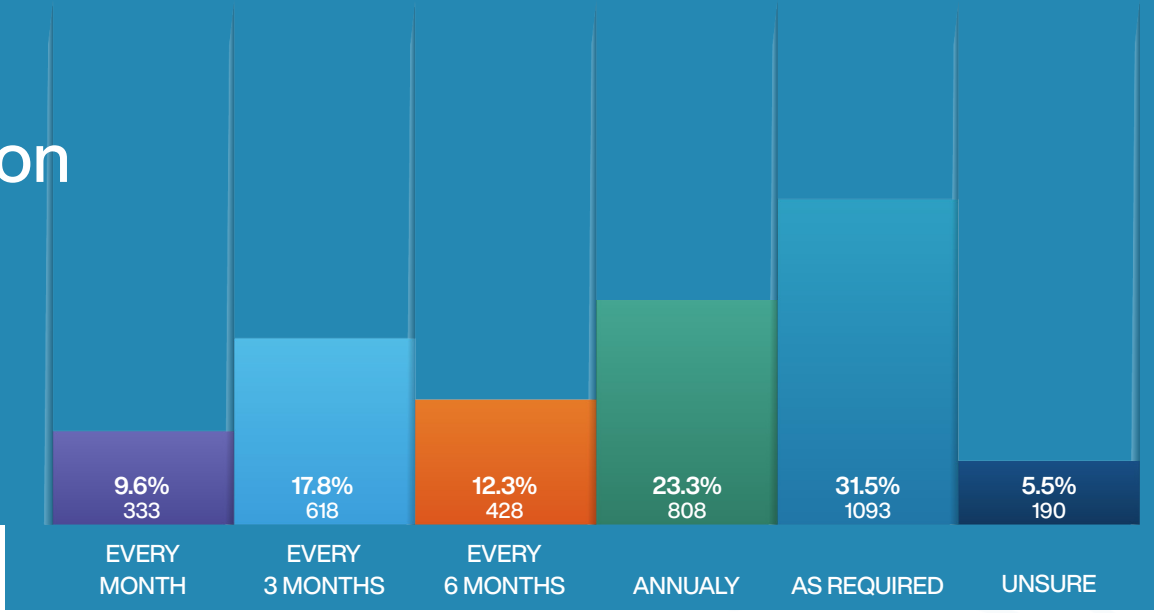
The survey underscores the need for a systematic approach to third-party cybersecurity management, including the establishment of clear contractual requirements, regular audits, and adherence to recognized standards. The data also indicates a potential need for industry-wide frameworks and guidelines that could support organisations in implementing robust third-party cybersecurity assessment practices.

The survey results highlight a critical area of cybersecurity that requires immediate attention and action. Ensuring the security compliance of third-party suppliers is not just a best practice but a necessity in an era where organisational boundaries are increasingly porous, and security is only as strong as the weakest link in the supply chain.



Question:

How often does your organisation conduct cyber security awareness training?



The survey provides further granularity on the frequency of cybersecurity awareness training across different organisations.

According to the survey:

- **9.59% conduct training every month,**
- **17.81% every 3 months,**
- **12.33% every 6 months,**
- **23.29% annually,**
- **31.51% as required,**
- **while 5.48% remain unsure of their training frequency.**

In light of the previous statistic that a majority of organisations had conducted some form of training in the last six months, this new data adds depth to our understanding of the training cadence. A proactive 9.59% of organisations prioritize cybersecurity to the extent of conducting monthly training sessions, reflecting a commitment to maintaining a high level of awareness among their staff.

Organisations conducting training quarterly or biannually represent a significant collective effort to keep cybersecurity front-of-mind, understanding that the threat landscape evolves rapidly enough to warrant frequent refreshers.

Interestingly, the largest single category of respondents conducts training 'as required,' which may suggest an adaptive approach to training frequency, potentially triggered by changes in the threat environment, updates to company policy, or in response to specific incidents.

However, there remains a notable portion of organisations that only conduct annual training or are unsure about their training frequency. While annual training is beneficial, the dynamic nature of cyber threats arguably necessitates more frequent updates to ensure staff are aware of the latest risks and strategies to mitigate them.

The uncertainty reported by 5.48% of respondents about the frequency of training could indicate a lack of formalized training schedules or policies within those organisations, which could lead to inconsistencies in staff cybersecurity awareness and preparedness.

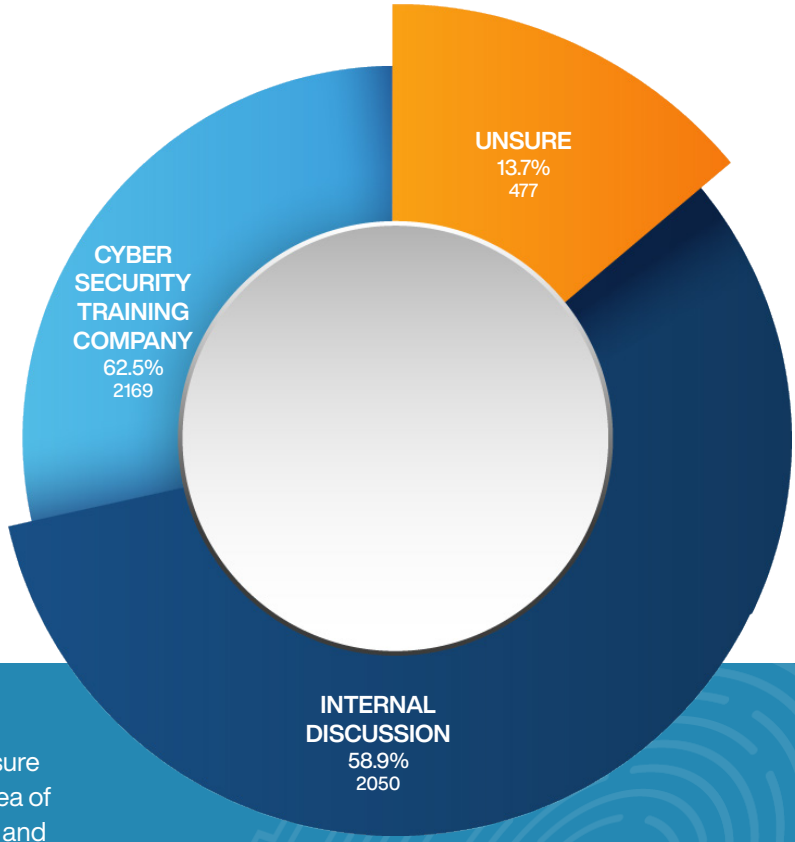
While there is a clear recognition of the importance of cybersecurity awareness training reflected in the data, there is still a need for many organisations to establish more regular and structured training programs. The goal should be to create a culture of continuous learning and vigilance to effectively counter the ever-evolving cyber threat landscape.

Question:

How do you conduct cyber security awareness training?

The survey sheds light on he methods through which organisations conduct cybersecurity awareness training.

A majority, 58.90%, rely on internal discussions for conducting such training. Meanwhile, 27.40% of organisations engage a cybersecurity training company, and 13.70% are unsure of how their training is conducted.



The prevalence of internal discussions as the primary mode of cybersecurity training could indicate a trend towards in-house capacity building and leveraging existing knowledge. This approach has the potential advantage of being tailored to the specific context and needs of the organisation. However, it may also suggest a limitation in accessing external expertise and a comprehensive understanding of cybersecurity threats and best practices.

The utilization of specialized cybersecurity training companies by over a quarter of respondents underscores a recognition of the value that external expertise can bring to an organisation's cybersecurity preparedness. These companies can offer structured training programs, up-to-date information on emerging threats, and best-practice responses.

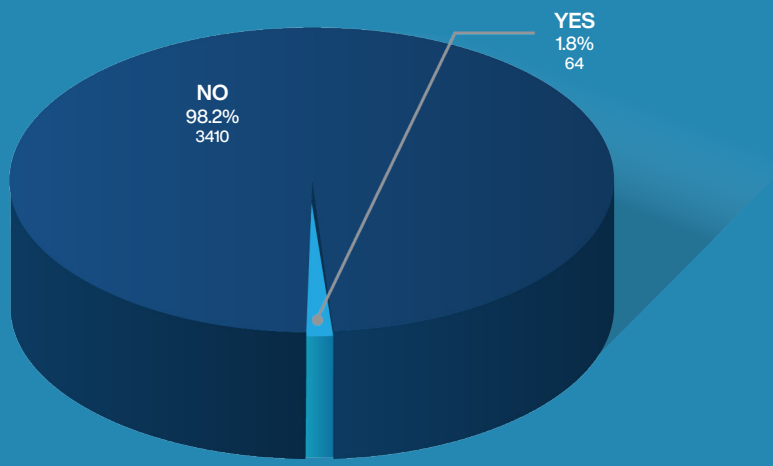
The proportion of respondents who are unsure about their training methods points to an area of concern. It suggests a lack of clear strategy and communication regarding cybersecurity training within these organisations, which may affect the effectiveness of their cybersecurity posture.

Considering the earlier statistics on the frequency and review of cybersecurity capabilities, this data reinforces the need for a strategic and informed approach to cybersecurity training. It is imperative for organisations to not only conduct training regularly but also to be deliberate about the training methods they employ. Whether choosing to build internal expertise or outsource to specialized firms, the goal should be to ensure that all employees are equipped with up-to-date knowledge to protect against and respond to cyber threats effectively.

Question:

Have you fully tested your cyber incident response plan with an external organisation?

The survey responses here highlight a critical shortfall in cybersecurity readiness across surveyed industries. When considering that only 22.10% of respondents have a written cyber incident response plan, the additional data point that a mere 1.84% have fully tested their plans with an external organisation is even more alarming.



This starkly low percentage of external testing indicates a significant vulnerability in the practical readiness of organisations to manage cyber incidents. The process of testing an incident response plan with an external entity is not merely a step towards validation, but also a crucial exercise in identifying weaknesses and improving response capabilities. It provides an objective assessment of how an organisation's plan stands up to scrutiny and can adapt to the evolving tactics of cyber adversaries.

Given the scant number of organisations that have a written plan in the first place, it follows that even fewer would have reached the stage of full external testing.

This gap points to a widespread trend of underpreparedness that transcends sectors and sizes of businesses. It suggests that, while some organisations may recognize the theoretical importance of incident response planning, the practical application and validation of these plans are not being prioritized.

The lack of external testing could be attributed to several factors. For many organisations, particularly SMBs, the resources and expertise required to conduct such testing may be lacking. There may also be a degree of complacency, with some organisations perhaps overestimating the efficacy of their in-house testing or underestimating the complexity of real-world cyberattacks. For larger entities, the challenge may lie in the coordination of complex and distributed systems, making comprehensive testing a significant undertaking.

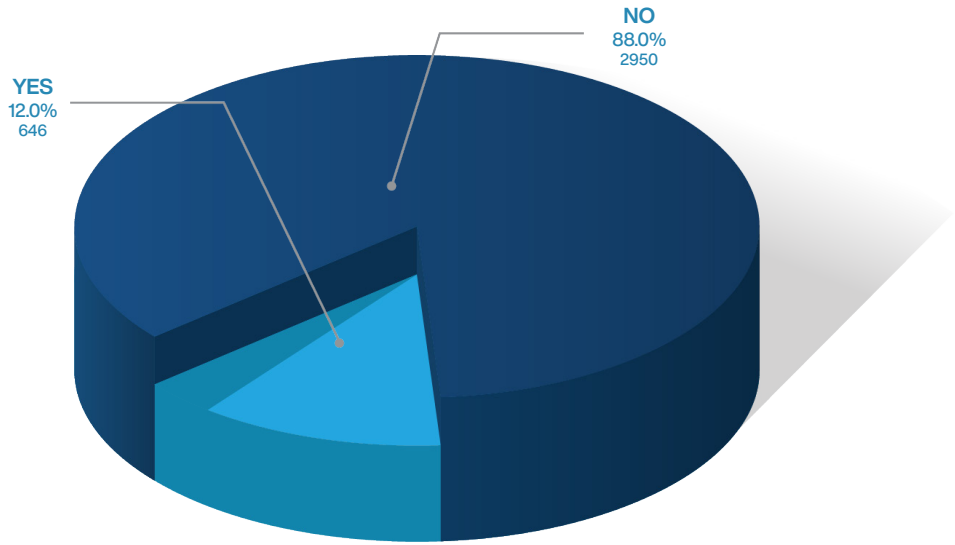
However, the benefits of external testing are clear. It can uncover blind spots that internal teams may overlook and provide valuable insights into an organisation's incident response efficacy from an attacker's perspective. It also prepares teams for the stress and unpredictability of an actual cyber incident, which cannot be fully replicated by internal exercises alone.

The survey data serves as a clarion call for industries to not only establish and document cyber incident response plans but also to ensure these plans are robustly tested and verified. This may involve leveraging partnerships for cybersecurity expertise, investing in regular external audits and simulations, and cultivating a culture that values and understands the critical role of cybersecurity in maintaining operational integrity.

In essence, the path to resilience in cyber incident management is a continual process that requires both the creation of comprehensive plans and the rigorous testing of these plans against real-world scenarios. As cyber threats continue to escalate in sophistication and impact, the necessity for such preparedness has never been more imperative.

Question:

Does your organisation have a cyber insurance policy?



The survey reveals that only a small percentage of organisations, 12.03%, have a cyber insurance policy in place.

This low uptake suggests that the vast majority of organisations, at 87.97%, may be underestimating the financial risks associated with cyber incidents or may find themselves potentially unprepared to deal with the repercussions of a cyberattack.

Cyber insurance can be a critical component of an organisation's risk management strategy, providing a safety net that can help mitigate the financial impact of data breaches, business interruption, and network damage. The fact that such a large proportion of organisations are operating without this protection is a cause for concern, especially in light of the high rates of password reuse and other security vulnerabilities identified in the survey data.

This gap in cyber risk preparedness could be due to a variety of factors, including a lack of awareness of the availability and benefits of cyber insurance, perceived cost barriers, or the complexity of cyber insurance policies. It may also reflect a general mindset of optimism bias, where organisations underestimate the likelihood or potential impact of cyber threats.

Given the ever-increasing cyber threat landscape, it is crucial for organisations to reconsider their stance on cyber insurance as part of a comprehensive cybersecurity strategy. Cyber insurance not only offers financial protection but also often provides access to support services in the event of a cyber incident, which can be invaluable in navigating the aftermath of an attack.

In conclusion, the survey data points to a significant opportunity for the cyber insurance industry to educate the market on the value of such policies. It also serves as a reminder for organisations to evaluate all aspects of their cybersecurity posture, including risk transfer mechanisms like insurance, to ensure comprehensive protection against the multifaceted nature of cyber risks.

Question:

Do you have a document classification system in place?

(i.e. classification of data based on its level of sensitivity, value and criticality to your business, which assists with security controls for the protection of data)

The survey reveals that only 32.88% of organisations have a document classification system in place. This system is pivotal for determining the level of security controls needed to protect data based on its sensitivity, value, and criticality to an organisation's operations.

The fact that 67.12% of respondents do not have such a system is a significant concern.

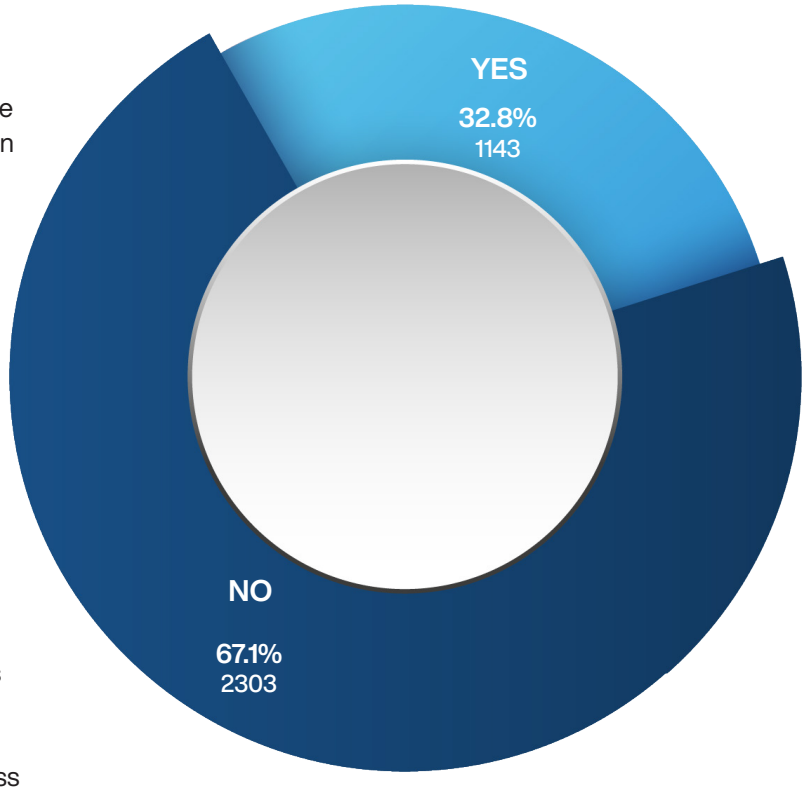
Document classification systems are fundamental to data security. Without them, organisations lack the structured approach necessary to allocate their security resources effectively. This could lead to critical data being insufficiently protected or resources being wasted on overprotecting non-sensitive information.

The lack of a document classification system may reflect broader trends in cybersecurity practice and awareness. For instance, smaller organisations may not have the expertise to implement such systems, or they may not recognize the value of classifying their data. Larger organisations might contend with the complexity of classifying large volumes of data and therefore may not have fully realized such systems.

The data from the survey suggests a need for a shift in how organisations perceive data protection. Classification systems should not be seen as an optional add-on but rather as an essential part of the cybersecurity infrastructure. They are the foundation upon which effective data protection protocols are built, ensuring that the most critical data receives the highest level of protection.

Moreover, the survey indicates a potential area of growth for cybersecurity service providers. There is an opportunity to assist organisations in understanding the importance of document classification and in implementing systems that can efficiently classify data at scale.

The low adoption rate of document classification systems highlights a gap in data security practices that could be mitigated through increased awareness, education, and the provision of scalable solutions tailored to the needs of organisations of varying sizes and complexities. Addressing this gap is crucial for bolstering the overall cybersecurity posture of organisations across industries.



Question:

When was the last time your organisation conducted Cyber Security awareness training?

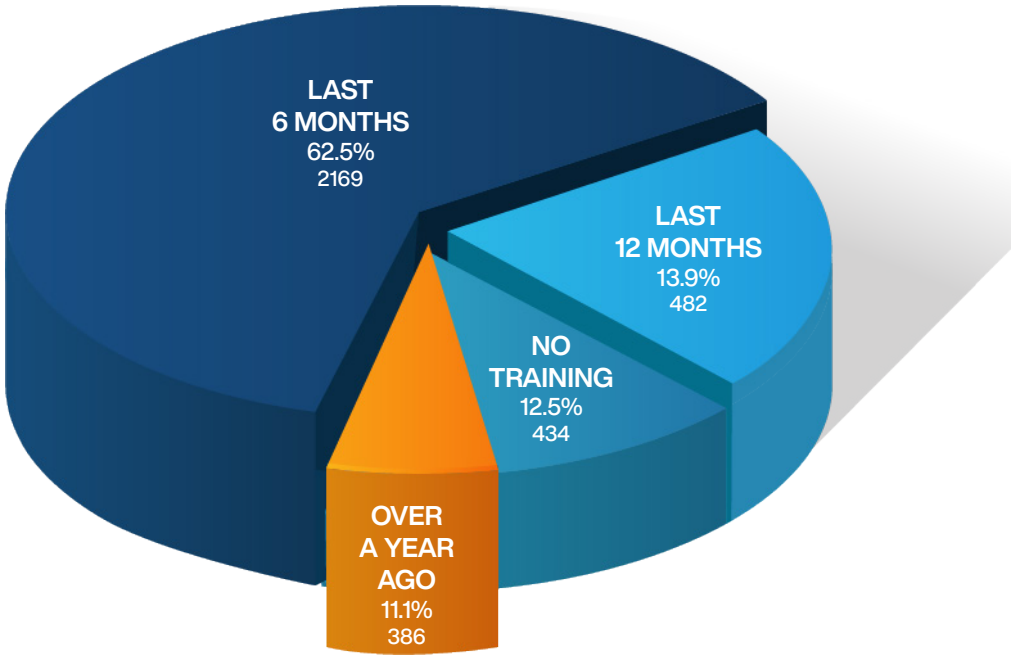
The survey reveals that a majority of organisations, 62.50%, have conducted cybersecurity awareness training within the last 6 months. This is a positive indication that cybersecurity awareness is being taken seriously by a substantial portion of the survey's respondents, recognizing the critical importance of keeping staff informed and vigilant against cyber threats.

However, the data also shows that a smaller yet significant percentage of organisations, 13.89%, have only conducted training within the last year, and 11.11% have not engaged in such training for over a year. This suggests that there is room for improvement in maintaining regular training schedules, which is vital given the fast-paced evolution of cyber threats.

Alarmingly, 12.50% of the organisations report not having received any cybersecurity training yet. This lack of training is concerning as it leaves a sizeable portion of the workforce potentially unprepared to identify and respond to cybersecurity incidents, which could pose significant risks to organisational data and systems.

Continuous training is key to an effective cybersecurity posture, as the human element often represents the most significant vulnerability within any organisation. Regular training updates ensure that all personnel are aware of the latest threats and best practices for defense.

The survey data highlights the necessity for ongoing cybersecurity awareness initiatives across all organisations. It is imperative for those organisations that have not conducted recent training, or any at all, to prioritize and implement regular cybersecurity awareness programs to enhance their overall security posture and mitigate the risk of cyber incidents.



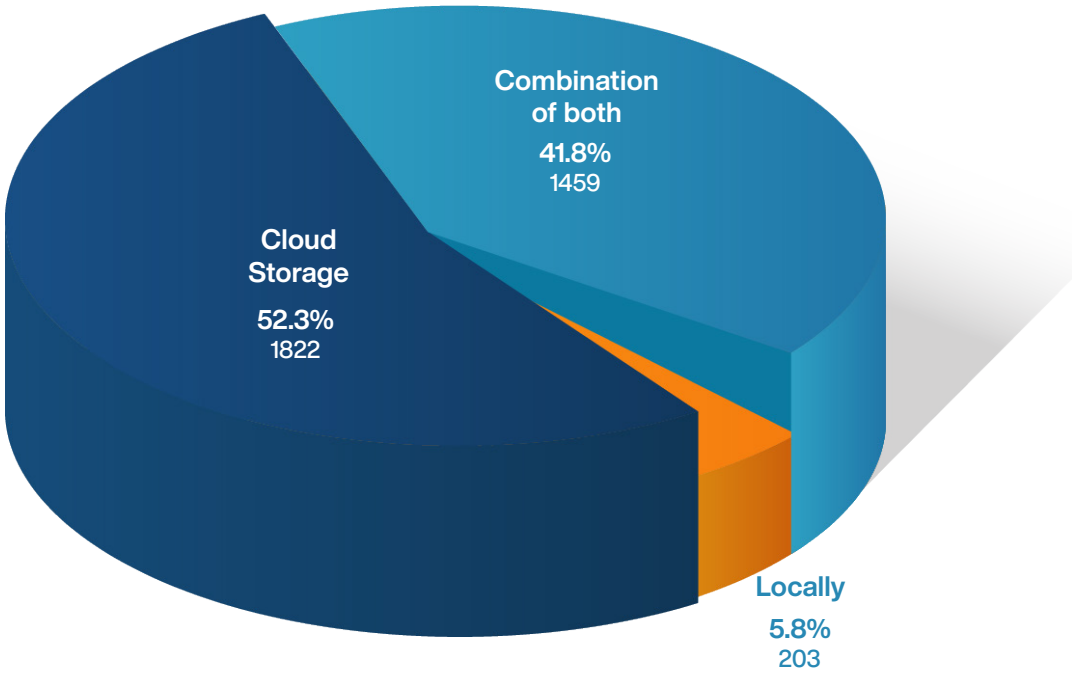

TECHNICAL
Username
REGISTER
LOGIN

Question:

At this time, where is your data stored?

The findings on data storage preferences among Australian organisations, coupled with the concerning statistics on password reuse and lack of MFA or 2FA usage, highlight the need for organisations to reassess their data security practices. To enhance their cybersecurity posture, businesses must focus on adopting strong security measures, such as unique and complex passwords, MFA or 2FA, and robust data protection policies, regardless of whether their data is stored locally, in the cloud, or a combination of both.

The data storage preferences of Australian organisations, revealing the following distribution: 5.83% (203) store their data locally, 52.30% (1822) use cloud storage, and 41.88% (1459) use a combination of both local and cloud storage. Taking into consideration that 98% of individuals surveyed reuse passwords and 92% do not employ multi-factor authentication (MFA) or two-factor authentication (2FA), this analysis aims to discuss the implications of these findings on the overall cybersecurity posture of these organisations.



Cloud storage preference

The majority of organisations (52.30%) store their data in the cloud, highlighting the growing trust in and reliance on cloud service providers. However, given that a large percentage of individuals reuse passwords and do not use MFA or 2FA, organisations must ensure that they implement strong security measures and best practices to protect their cloud-stored data.

Local storage risks

The 5.83% of organisations storing their data locally face unique cybersecurity challenges. The reuse of passwords and lack of MFA or 2FA implementation might pose even more significant risks for these organisations, as they may not benefit from the same level of security provided by reputable cloud service providers.

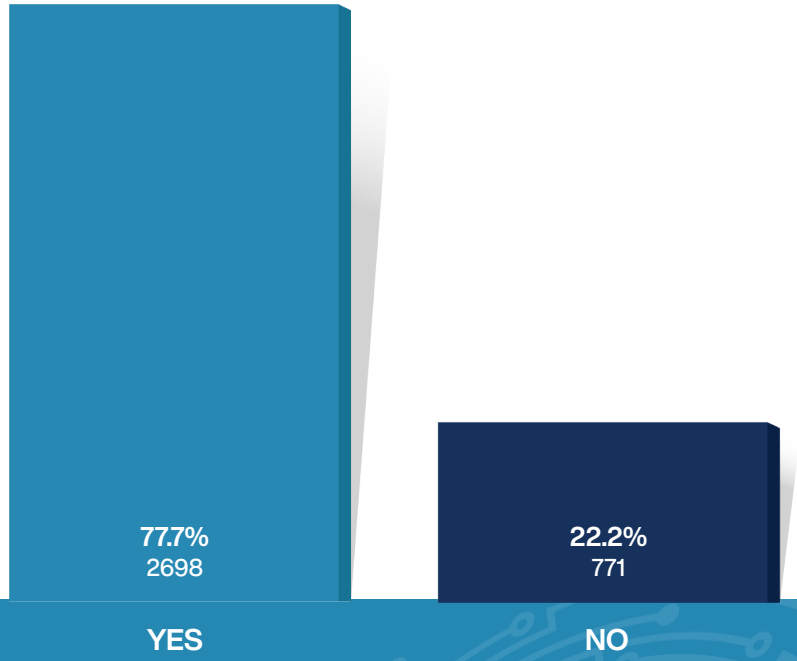
Combination storage complexities

The 41.88% of organisations using a combination of local and cloud storage must navigate the complexities of securing their data across both environments. The widespread reuse of passwords and lack of MFA or 2FA usage might further compound these challenges, as the organisations must implement robust security measures to protect their data in both locations.

Question:

Does your organisation currently use a Password Manager?

The data from survey indicates that a substantial majority of organisations, 77.78%, are utilizing a password manager. This adoption rate suggests a strong awareness of the foundational role that password security plays in an overall cybersecurity strategy.



Password managers are essential tools that enable users to maintain unique, complex passwords for different services without the need to remember each one. This can significantly enhance security by reducing the risk of password reuse across multiple platforms, a common vulnerability exploited in various cyber attacks.

However, the fact that 22.22% of organisations do not use a password manager reveals a potential area of risk. Organisations that do not employ password managers may be more susceptible to breaches resulting from compromised credentials. It is possible that these organisations might rely on less secure methods of password management, such as using simpler passwords or reusing them, which can be particularly hazardous in the event of a credential leak or phishing attempts.

Considering the earlier findings regarding the frequency and methods of cybersecurity training, the high usage of password managers could be reflective of the effectiveness of such training programs in imparting good password practices. Nonetheless, the survey data underscores the need for continued education and adoption of secure password practices, including the use of password managers, especially for the 22.22% of organisations that have yet to implement them.

In conclusion, while the survey shows a positive trend in the adoption of password managers, there remains a significant proportion of organisations that could improve their cybersecurity posture by incorporating such tools into their cybersecurity protocols.

Question:

Does your organisation monitor for reused passwords?

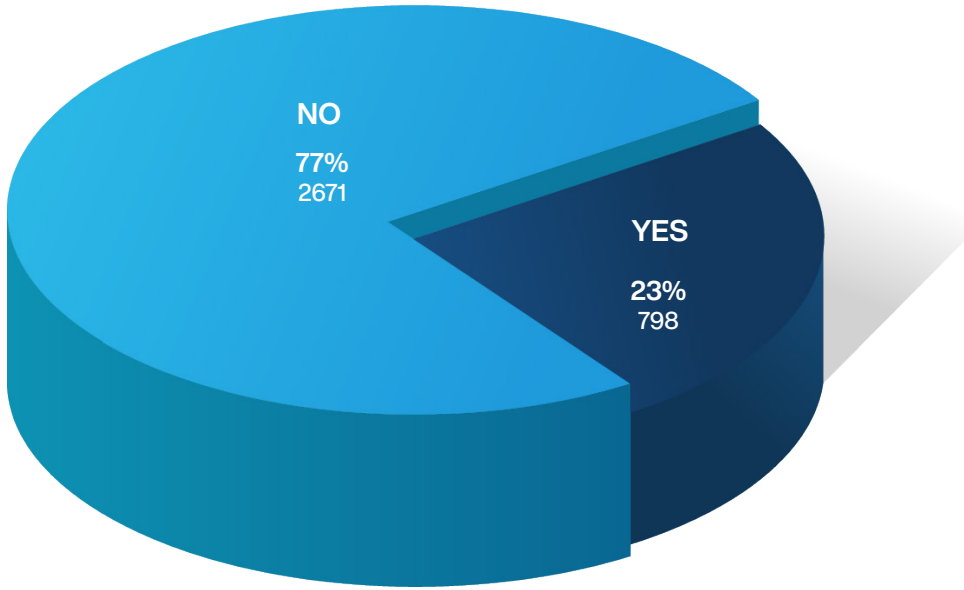
The survey reveals that only 23% of organisations actively monitor for reused passwords. This is a critical cybersecurity practice, and the fact that 77% of respondents do not engage in this monitoring is concerning.

Password reuse is a common but dangerous practice that significantly increases the risk of a security breach. If a set of credentials is compromised on one platform, any other accounts sharing the same credentials are also at risk. The act of monitoring for reused passwords is essential because it helps to enforce good password hygiene and reduces the vulnerability of accounts across different systems.

Given the earlier data showing a high adoption rate of password managers, the lack of monitoring for reused passwords presents a paradox. While many organisations facilitate the use of unique passwords through managers, they may not be taking the critical step of ensuring these tools' effective use by monitoring password reuse. This suggests a gap in the implementation of comprehensive password security measures.

The data underscores the need for organisations to not only adopt tools like password managers but also to actively monitor their use to prevent insecure practices. This should be part of a broader cybersecurity strategy that includes regular training, audits, and the establishment of protocols for secure password creation and management.

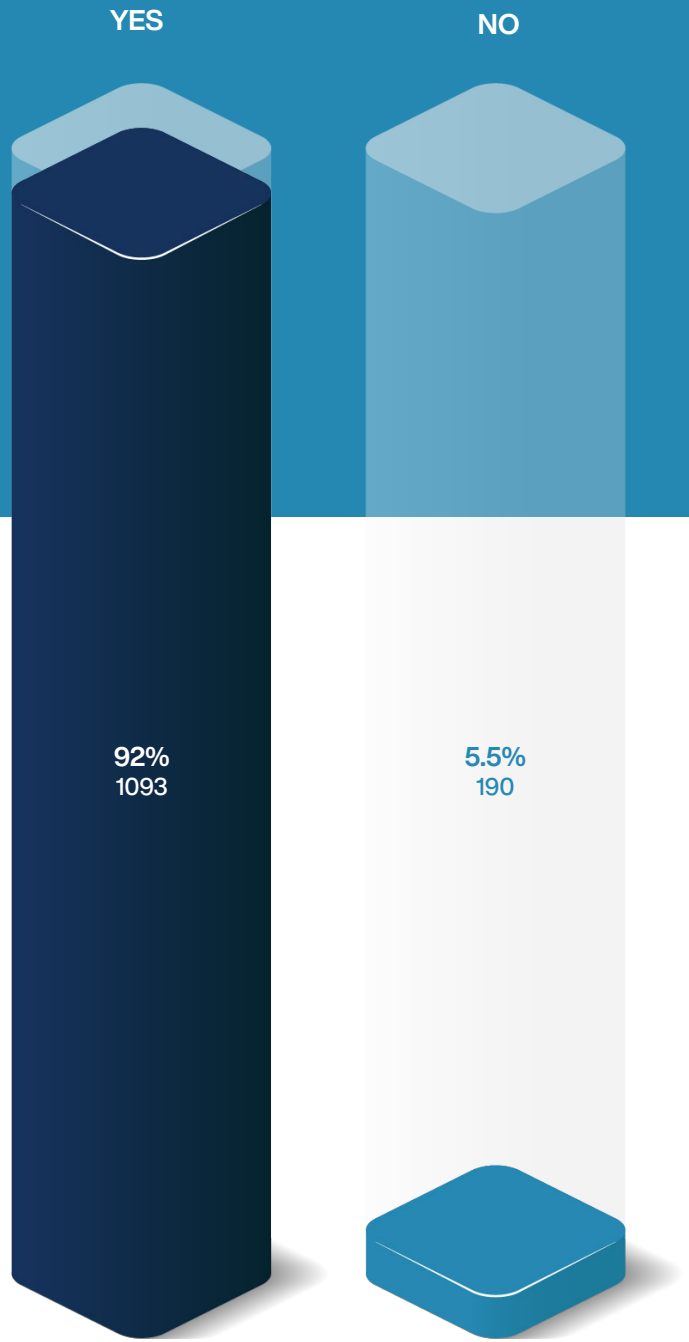
In conclusion, the survey highlights an area where many organisations could significantly improve their security posture.
By implementing monitoring for reused passwords, they can proactively address a common and potentially devastating security risk.



Question:

Do you reuse business and personal passwords?

The information from the 2023 State of Cyber Security Survey shows a strikingly high rate of password reuse among respondents, with 92% indicating they reuse business and personal passwords. This practice exposes both personal and professional systems to a higher risk of security breaches, as compromised credentials in one area can lead to unauthorized access in another.



This statistic is particularly alarming when juxtaposed with the earlier data indicating that while a significant proportion of organisations use password managers, a vast majority do not monitor for reused passwords. The inconsistency suggests that although tools to create and manage unique passwords are in place, their potential for improving security is not fully realized due to the continued practice of password reuse.

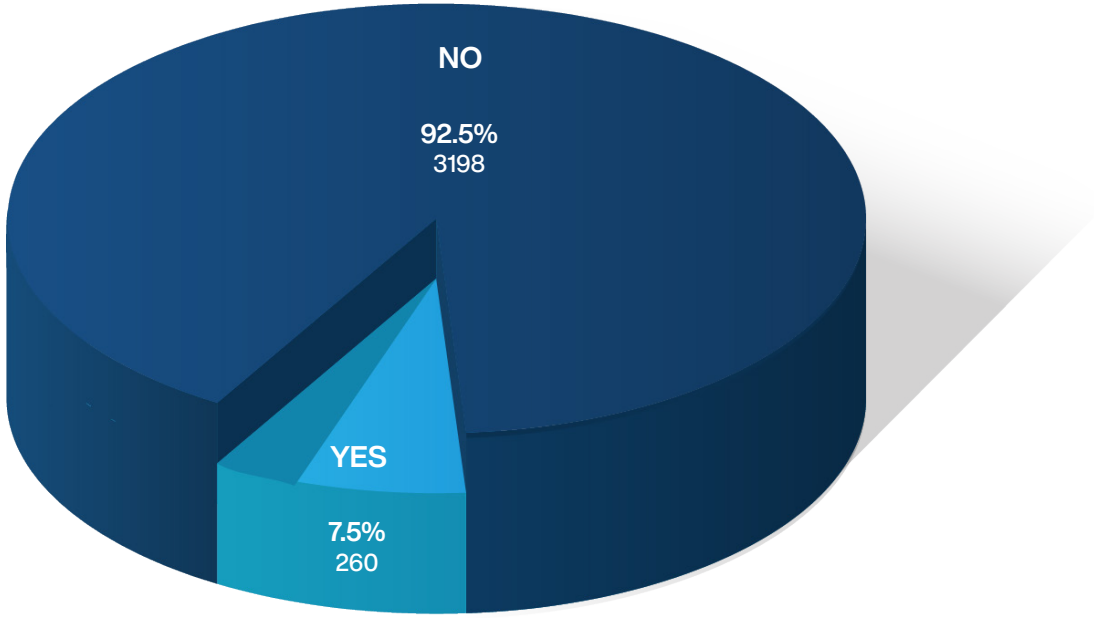
The data points toward a critical disconnect between the adoption of cybersecurity tools and the implementation of security best practices. It highlights the urgent need for more effective cybersecurity awareness training that emphasizes the risks associated with password reuse and guides individuals in both personal and professional contexts to adhere strictly to security protocols.

Addressing this widespread issue requires a concerted effort to shift behavior through ongoing education, the enforcement of strong password policies, and the use of technological solutions that can detect and prevent reused passwords across business and personal accounts.

In summary, the survey results reflect a substantial area of vulnerability within cybersecurity practices that must be urgently addressed. Organisations need to intensify efforts to educate about secure password practices and implement measures that can detect and mitigate the risks associated with password reuse.

Question:

Do you currently use 2FA or multifactor authentication on your email?



The findings on 2FA and MFA adoption among Australian organisations underscore the urgent need for businesses to prioritize implementing these essential security measures.

By adopting 2FA or MFA, organisations can better protect their sensitive information and systems from unauthorized access, reducing the likelihood of falling victim to cyberattacks and mitigating the potential damage caused by hackers and cybercriminals. It is crucial for businesses to recognize the importance of 2FA and MFA and take steps to implement these security practices to strengthen their overall cybersecurity posture.

The results revealed that 7.52% (260) of respondents use 2FA or MFA, while a staggering 92.48% (3198) do not. This analysis aims to discuss the implications of these statistics on the overall cybersecurity posture of these organisations and the potential impact on hackers and cybercriminals' activities.

Limited adoption of 2FA and MFA:

The fact that only 7.52% of organisations use 2FA or MFA highlights a significant gap in cybersecurity measures. 2FA and MFA are widely regarded as essential security practices to protect sensitive information and systems from unauthorized access, yet the vast majority of organisations are not employing these safeguards.

Increased vulnerability to hackers and cybercriminals:

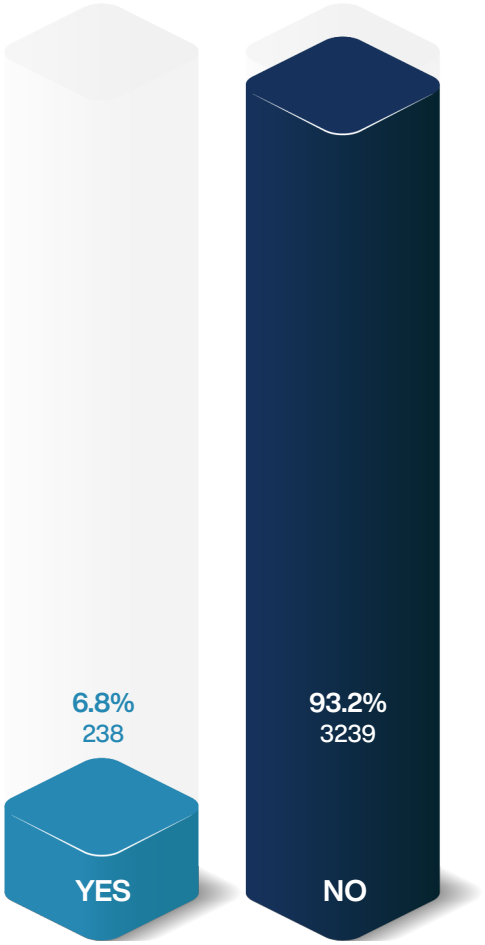
The 92.48% of organisations not using 2FA or MFA are at a higher risk of falling victim to cyberattacks, such as phishing, credential theft, and unauthorized access. Without the added layer of security provided by 2FA or MFA, hackers and cybercriminals can more easily exploit weak or stolen credentials, potentially leading to significant data breaches, financial losses, and reputational damage.

Increased vulnerability to hackers and cybercriminals:

The 92.48% of organisations not using 2FA or MFA are at a higher risk of falling victim to cyberattacks, such as phishing, credential theft, and unauthorized access. Without the added layer of security provided by 2FA or MFA, hackers and cybercriminals can more easily exploit weak or stolen credentials, potentially leading to significant data breaches, financial losses, and reputational damage.

Question:

Do you send business emails from personal accounts?



The findings on the use of personal accounts for sending business emails among Australian organisations emphasize the importance of adhering to best practices and using separate, professional email accounts for work-related correspondence.

By doing so, organisations can better protect their sensitive information and systems, reduce the likelihood of data breaches, and ensure compliance with relevant laws and regulations. It is crucial for businesses to recognize the potential risks associated with using personal accounts for business purposes and take steps to implement and enforce appropriate email usage policies to strengthen their overall cybersecurity posture.

The results revealed that 6.84% (238) of respondents use their personal accounts for business correspondence, while 93.16% (3239) do not. This analysis aims to discuss the implications of these statistics on the overall cybersecurity posture of these organisations and the potential risks associated with using personal accounts for business purposes.

Limited use of personal accounts for business emails

The majority (93.16%) of organisations do not use personal accounts for sending business emails, demonstrating that most businesses adhere to best practices by using separate, professional email accounts for work-related correspondence. This separation helps maintain the security and privacy of both personal and business information.

Increased risks for organisations using personal accounts

The 6.84% of organisations that use personal accounts for business emails expose themselves to increased cybersecurity risks. Personal email accounts may not be as secure as corporate accounts, which often have stricter security measures in place, such as encryption and stronger password requirements.

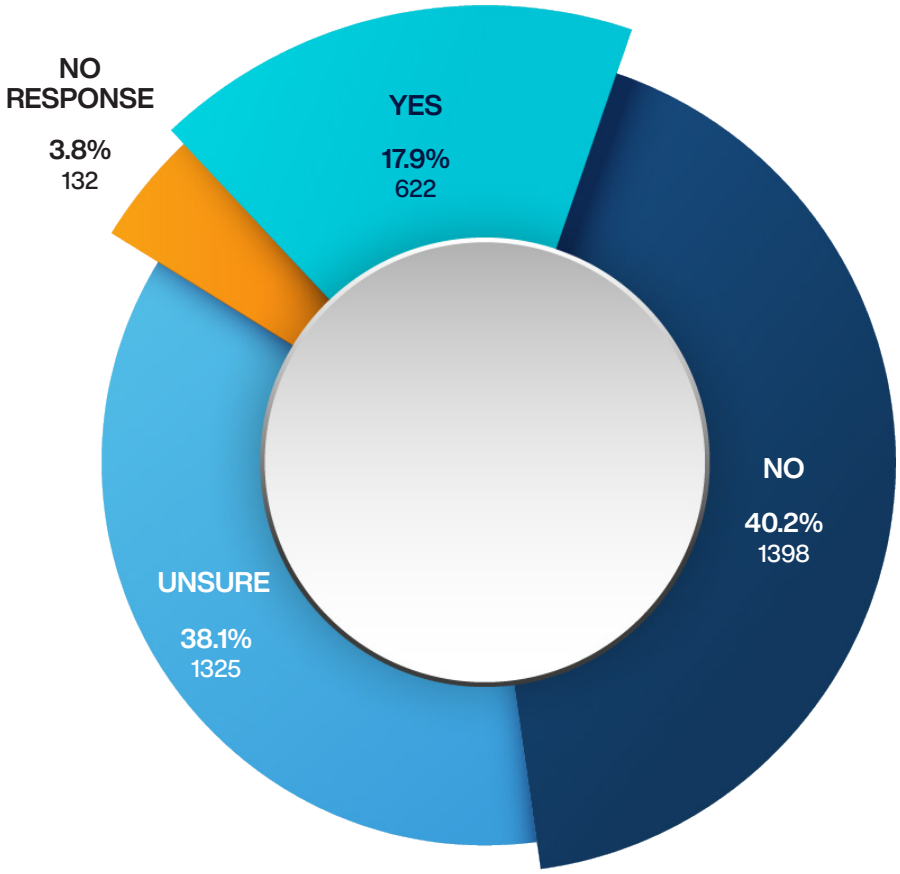
Additionally, using personal accounts for business purposes may lead to accidental data breaches, as confidential information may be more easily leaked or accessed by unauthorized individuals.

Legal and compliance concerns

Organisations using personal accounts for business emails may also face legal and compliance challenges. Confidential or sensitive information shared through personal accounts may not be properly protected, potentially violating data protection laws and regulations. Moreover, in the event of a legal dispute or investigation, accessing and preserving emails sent from personal accounts may be more complicated than obtaining emails from corporate accounts.

Question:

Do you use a Firewall within your Environment?



In summary, the data suggests that a considerable number of organisations may be operating without the fundamental cybersecurity protection that firewalls provide, or there is a significant lack of awareness about security infrastructure and practices.

This lack of firewall implementation or knowledge thereof poses a substantial risk and underscores the need for improved cybersecurity awareness and infrastructure implementation. Organisations should be advised to verify their network security measures and consider investing in firewalls if they haven't already, as well as improving cybersecurity education across their staff to ensure everyone understands the security measures in place.

The statistics provide an overview of the use of firewalls within various organisations' environments:

Firewall Usage:
A minority of respondents, less than one-fifth, confirm the use of a firewall within their environments. This percentage represents organisations that have taken a fundamental step in protecting their network perimeters.

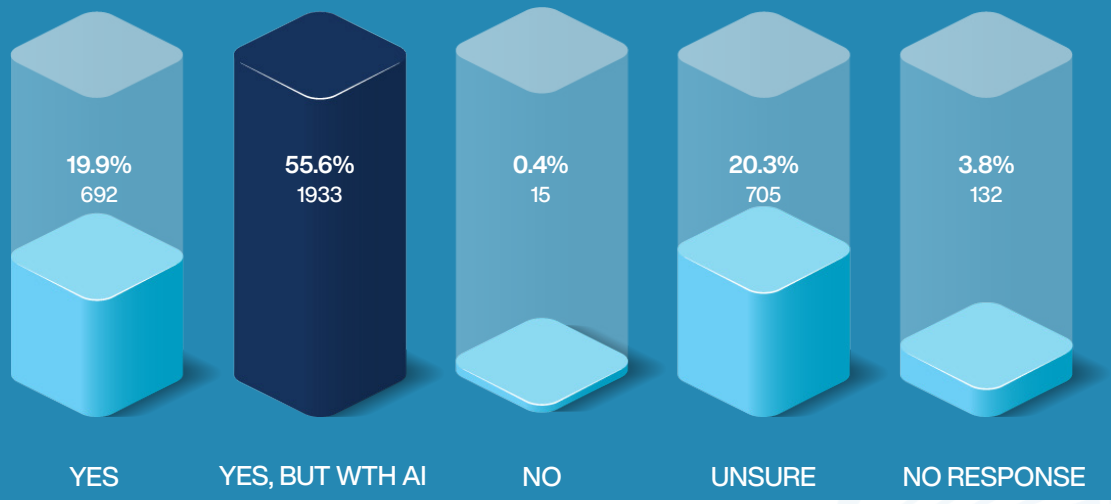
No Firewall:
Surprisingly, over two-fifths of the respondents indicate that they do not use a firewall. This is a significant security concern, as firewalls are a basic and essential line of defence against external threats.

Uncertainty about Firewall Usage:
A large proportion of respondents are unsure if they have a firewall in place. This level of uncertainty suggests a lack of clarity or communication regarding security infrastructure, which may reflect a wider issue of inadequate cybersecurity governance.

Non-Response:
A small fraction did not respond to the question, which might indicate a lack of knowledge about their security measures or an oversight in responding to the survey.

Question:

Do you utilise End Point Protection with AI integrated?



The statistics provide insight into the deployment of endpoint protection among various organisations:

Standard Endpoint Protection (19.90%):
A fifth of the respondents use standard endpoint protection. This indicates that these organisations have taken steps to protect their devices from malware and other security threats, which is a critical aspect of cybersecurity.

Endpoint Protection with AI (55.59%):
Over half of the organisations surveyed are utilising endpoint protection that incorporates AI. This suggests a significant adoption of more advanced, intelligent systems capable of predicting, identifying, and responding to threats more efficiently than traditional methods.

No Endpoint Protection (0.43%):
Only a very small fraction report not using any form of endpoint protection. This is exceptionally risky, as unprotected endpoints can easily be compromised, leading to potential data breaches and other security incidents.

Uncertainty About Protection (20.28%):
Notably, over a fifth of respondents are unsure about whether they utilise endpoint protection. This uncertainty could indicate a lack of direct involvement in cybersecurity efforts or a communication gap within these organisations.

No Response (3.80%):
A small percentage did not respond to the question, which might suggest a lack of engagement with the topic or a lack of awareness of their security posture.

In summary, the data suggests that a significant number of organisations are embracing advanced endpoint protection solutions with AI capabilities, reflecting a trend towards intelligent cybersecurity defences.

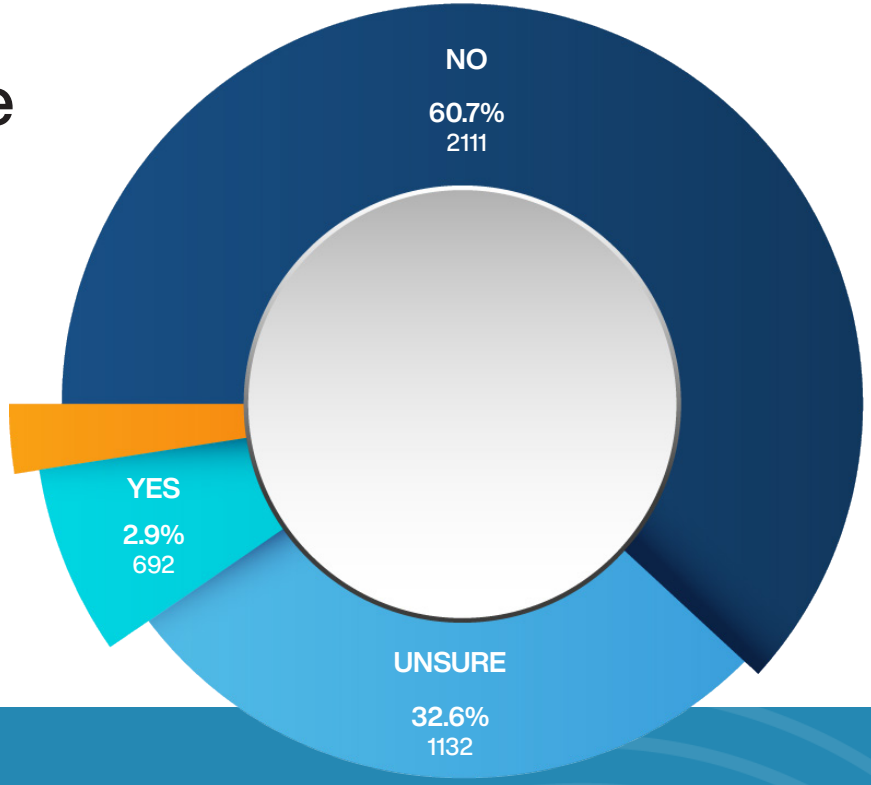
However, the level of uncertainty reported by many respondents highlights the need for better education and communication regarding cybersecurity measures within organisations. It's crucial for all organisations to be aware of and understand the security tools they have at their disposal to protect against the evolving landscape of cyber threats effectively."

Question:

Does your End Point Protection integrate with our cyber security technologies?

(e.g SIEM, SOAR, Threat Intelligence Platforms)

The statistics indicate how well endpoint protection is integrated with other cybersecurity technologies in organisations:



Integration Present (2.93%):
A very small proportion of respondents (102) indicate that their endpoint protection is integrated with other cybersecurity technologies like SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), or Threat Intelligence Platforms. Integration is critical for a cohesive security posture as it allows different tools to work together for more effective threat detection and response.

No Integration (60.71%):
The majority of respondents (2111) state that their endpoint protection does not integrate with other cybersecurity technologies. This suggests that many organisations may be missing out on the benefits of a unified security approach, potentially leading to silos that can hamper the effectiveness of their cybersecurity efforts.

Uncertainty About Integration (32.56%):
A significant number of respondents (1132) are unsure if their endpoint protection integrates with other cybersecurity tools. This uncertainty can reflect a lack of visibility or understanding of the security infrastructure, which can be detrimental to the organisation's ability to respond to cyber threats promptly.

No Response (3.80%):
A small portion did not respond, which may indicate a lack of knowledge or engagement with their organisation's cybersecurity strategy.

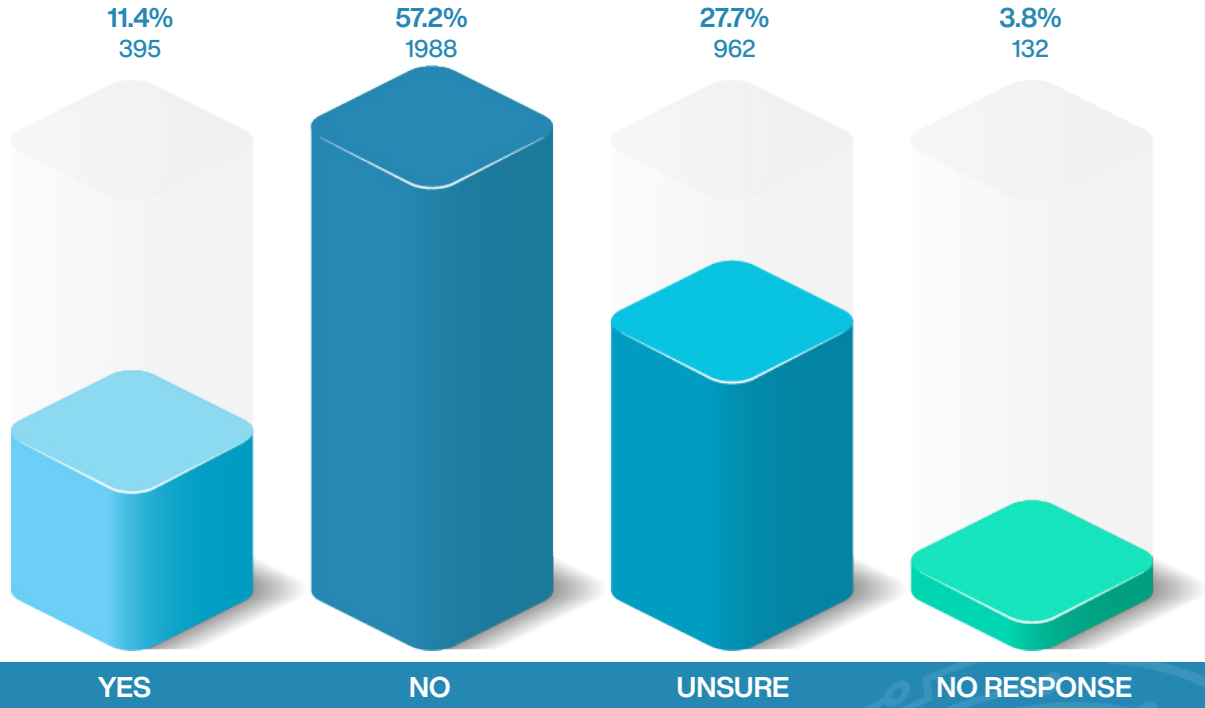
In summary, the data reveals a notable gap in the integration of endpoint protection with other cybersecurity technologies within a large number of organisations. This lack of integration could lead to inefficiencies and vulnerabilities in an organisation's cybersecurity defences. It emphasises the need for improved cyber security strategies that promote better integration of tools and technologies to enhance overall security resilience. Additionally, the high level of uncertainty suggests that there is a considerable opportunity for education and better communication regarding the cyber security infrastructure in place.

Question:

Does your environment utilise MDM?

(Mobile Device Management)

The data reflects the adoption and awareness of Mobile Device Management (MDM) within organisations:



MDM Adoption (11.36%):
A small percentage of the respondents (395) state that they utilise MDM in their environments. MDM is essential for managing and securing an organisation's mobile devices and ensuring that they comply with the company's security policies.

No MDM Usage (57.18%):
A majority of respondents (1988) report not using MDM. This indicates that over half of the surveyed organisations may be at risk of security breaches stemming from unmanaged mobile devices, which can be a significant vulnerability given the increasing reliance on mobile technology in the workplace.

Lack of MDM Knowledge (27.67%):
A substantial number of respondents (962) do not know what MDM is. This lack of awareness highlights a significant gap in knowledge that could prevent these organisations from taking advantage of MDM's benefits for securing mobile devices.

No Response (3.80%):
A small portion of the sample did not provide an answer, which may point to a lack of engagement with the concept of mobile device security or potentially indicate respondents who are not involved in their organisation's cybersecurity decision-making.

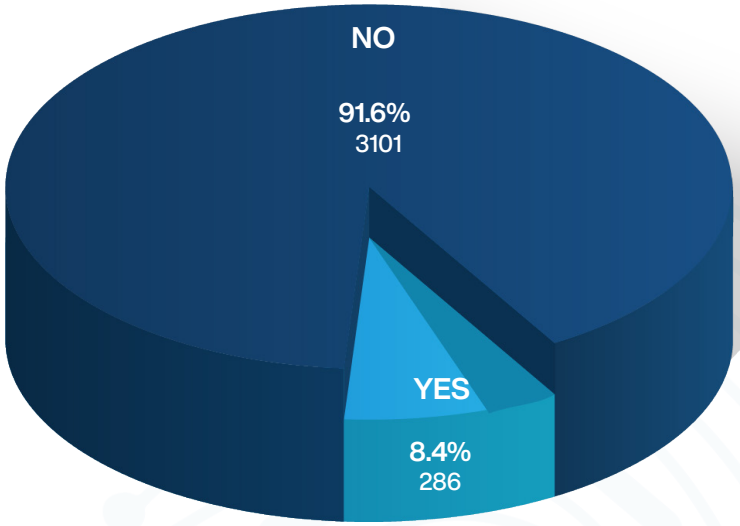
In summary, the data suggests that MDM is not widely implemented or understood among a large number of organisations. Given the prevalence of mobile devices in the business environment and their potential as a security risk, the low adoption and awareness rates of MDM solutions call for an increased focus on mobile security.

Organisations should be educated about the importance of MDM in protecting sensitive information, especially in an era of growing mobile usage, remote work, and BYOD (Bring Your Own Device) policies. Enhancing MDM adoption could significantly bolster the overall cybersecurity posture by extending protections to mobile endpoints.

Question:

Have you ever performed a penetration test?

A penetration test is an authorised simulated cyber attack on your computer system, performed to evaluate the security of the system.



The empirical evidence demonstrates a disparate level of engagement in penetration testing across various sizes and types of organisations, suggesting a nuanced landscape where resource allocation and the intrinsic nature of cloud environments play significant roles.

It is essential to acknowledge that small and medium-sized businesses (SMBs) often operate with limited resources, both in terms of financial capacity and cybersecurity expertise. This scarcity impacts their ability to implement comprehensive security measures, including penetration testing. Consequently, the low percentage of SMBs conducting such tests is not merely a reflection of negligence, but rather an indication of the constraints within which these businesses operate. Furthermore, the prevalence of cloud-based solutions in this cohort, often provided by third parties that conduct their own penetration testing, might contribute to a false sense of security, leading these businesses to deprioritize additional independent security assessments.

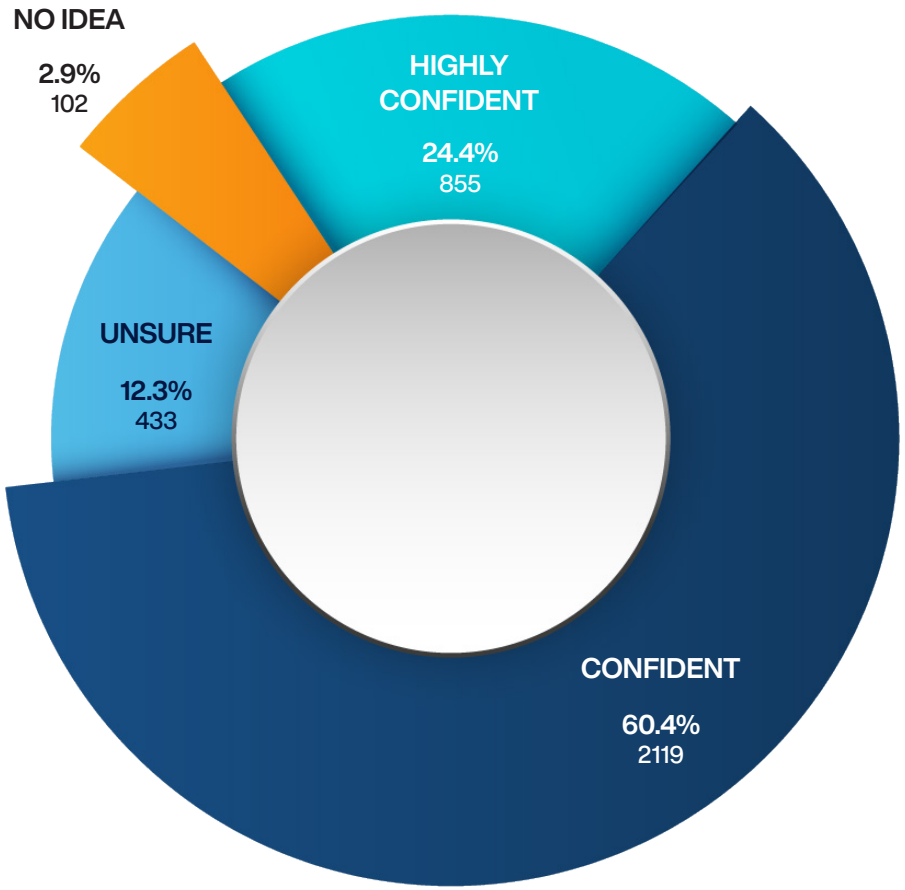
Larger organisations, however, particularly those operating within complex hybrid and on-premises environments, manifest a different scenario. The assumption that penetration testing conducted by software developers is sufficient for security assurance does not hold the same weight in these contexts.

Given the intricate and customized nature of their digital infrastructure, these entities cannot rely solely on third-party assessments. The data suggests a concerning trend wherein such organisations, despite having greater resources, are not uniformly engaging in penetration testing. This is a significant oversight, as the complexity and customization inherent in larger systems introduce a myriad of potential vulnerabilities that are best identified through rigorous and regular penetration testing.

The survey's data accentuates the need for a stratified approach to cybersecurity, one that recognizes the diversity of organisational capabilities and the varying degrees of control over digital environments. For SMBs, the path forward may involve a greater reliance on cloud service providers and a need for industry-wide standards that ensure these providers uphold stringent security practices. For larger organisations, the data serves as a call to action to leverage their resources to conduct thorough penetration testing, especially in less centralized and more complex IT environments.

Question:

How confident are you at being able to identify Phishing emails?



Our survey highlights a promising trend of heightened awareness among participants regarding the identification of phishing emails. A substantial 84.76% of respondents exhibit confidence, with 24.37% asserting high confidence and 60.39% expressing general confidence. This data may reflect the positive impact of cybersecurity awareness campaigns and educational programs that aim to equip the public with the knowledge and skills necessary to recognize and avoid cyber threats.

However, the presence of 12.34% of respondents who are unsure and 2.91% who have no idea about their ability to identify phishing emails underscores a crucial opportunity for further educational outreach. It's essential to address this gap with targeted educational initiatives that are inclusive of all levels of proficiency and adaptable to various learning preferences.

The survey also brings to light the potential issue of overconfidence. Confidence does not inherently guarantee the ability to identify sophisticated phishing attempts accurately. This discrepancy between perceived and actual skill levels can lead to a false sense of security, potentially making individuals susceptible to more complex phishing schemes. Cybersecurity training programs should, therefore, aim to challenge this overconfidence by incorporating practical exercises that simulate real-life phishing scenarios and by continuously updating content to reflect the latest threat landscape.

In light of the rapidly evolving nature of cyber threats, the need for ongoing education cannot be overstated. Phishing techniques are becoming more advanced, often bypassing conventional detection methods. Lifelong learning is thus imperative for individuals to remain vigilant and prepared to counteract these threats effectively.

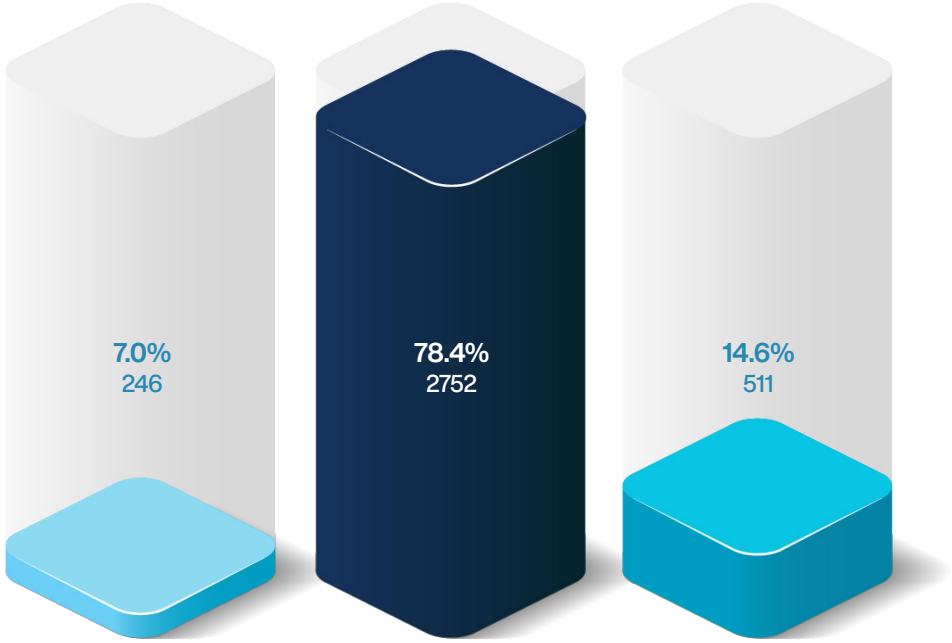
Furthermore, the psychological aspects of cybersecurity, such as cognitive biases, play a significant role in individual confidence levels. Recognizing and addressing these biases within cybersecurity training can lead to more accurate self-assessment and improved preparedness among users.

In summary, while the reported levels of confidence are encouraging, they highlight the necessity of continuous, adaptive, and psychologically-informed cybersecurity education. This approach will ensure that confidence is not only maintained but is also matched by the ability to effectively counter increasingly sophisticated cyber threats.

Question:

Do you report Phishing emails when recognised?

The data presented here paints a concerning picture about the reporting behaviors related to phishing emails. Despite a previous indication that a majority of respondents are confident in identifying phishing emails, a substantial 78.43% admit they do not report phishing emails when recognized. This disparity raises significant questions about the effectiveness of cybersecurity awareness and the actual practices of email users.



The data presented here paints a concerning picture about the reporting behaviors related to phishing emails. Despite a previous indication that a majority of respondents are confident in identifying phishing emails, a substantial 78.43% admit they do not report phishing emails when recognized. This disparity raises significant questions about the effectiveness of cybersecurity awareness and the actual practices of email users.

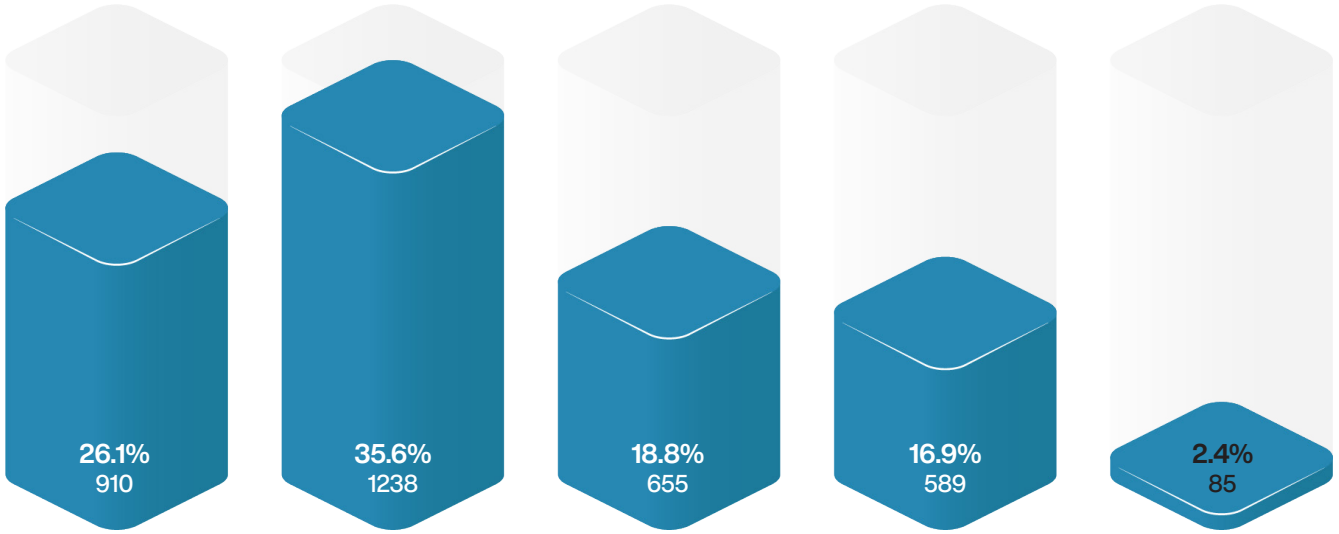
Only a small fraction, 7.01%, consistently take the proactive step of reporting recognized phishing attempts. This low reporting rate is alarming as it suggests that even when users can identify phishing emails, most are not engaging in best practices to help mitigate the spread and impact of such attacks. Reporting phishing attempts is a critical step in cybersecurity as it helps organizations to update their security measures and alert other users to the threat.

The 14.56% of respondents who sometimes report phishing attempts may represent occasional vigilance, but it also indicates a lack of consistent behavior in addressing cybersecurity threats.

Question:

Do you restrict access to information internally?

The data reflects the internal information access control practices among various organisations:



In summary, while a majority of organisations implement some form of access restriction, a concerning number either do not restrict access or are unsure of their access control policies. This highlights a potential area for improvement, as effective access control is a cornerstone of information security. Organisations should aim to ensure that access to sensitive information is appropriately restricted and that all staff are aware of and understand the access control policies in place.

Full Restriction:
Over a quarter of the respondents indicate that they always restrict access to information within their organisations. This suggests a comprehensive approach to information security, with access likely governed by strict policies and controls.

Partial Restriction:
The largest segment of respondents apply partial restrictions. This could imply role-based access control where employees have access to information necessary for their specific roles, a practice that balances operational efficiency with security.

No Restriction:
Nearly one-fifth report no restrictions on internal information access. This is concerning as unrestricted access can increase the risk of data breaches, either accidental or malicious.

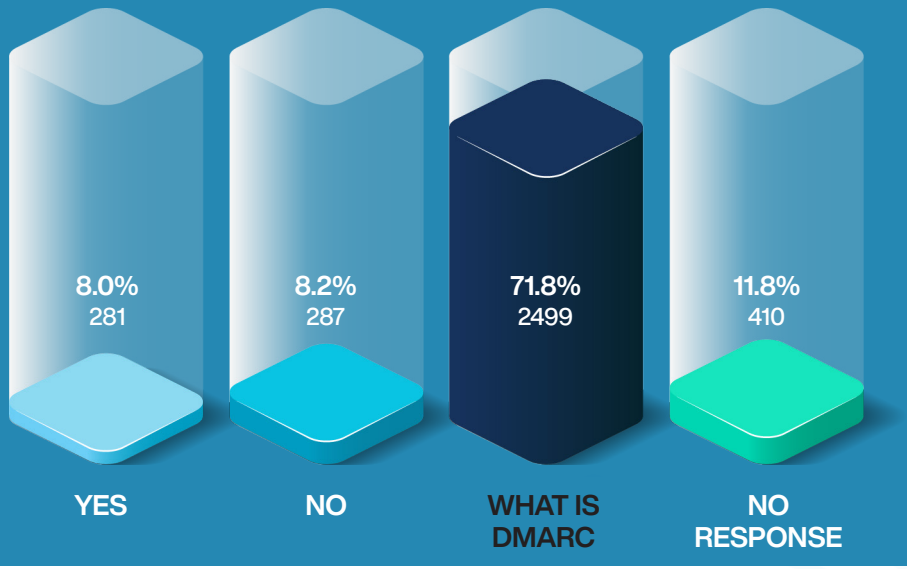
Uncertainty:
A significant number of respondents are unsure about their information access policies. This uncertainty can lead to inconsistent application of access controls and may indicate a need for clearer communication and policy enforcement within these organisations.

No Response:
A small percentage did not respond, which could suggest a lack of engagement with the policy or a possible lack of awareness of access control practices.

Question:

Does your Business utilise DMARC to prevent domain spoofing?

The data concerning the use of DMARC (Domain-based Message Authentication, Reporting, and Conformance) for preventing domain spoofing among businesses reveals several notable points:



Implications for Cybersecurity Awareness and Practices:
Urgent Need for Education: The fact that the majority of respondents do not know what DMARC is suggests an urgent need for increased education on cybersecurity practices, particularly around email security.

Potential for Increased Phishing Vulnerability:
Without widespread adoption of DMARC, businesses may be more susceptible to domain spoofing and phishing attacks, which are common vectors for cybersecurity breaches.

Importance of Email Security in Cyber Defence:
Given that email is a common attack vector, the lack of DMARC adoption points to a potential weakness in overall cybersecurity defences among businesses.

Possible Overlook in Cybersecurity Strategies:
The data may indicate that email authentication measures like DMARC are being overlooked in cybersecurity strategies, which could be a point of focus for improvement.

Recommendations for Research and Strategy Development:

Advocacy for DMARC Implementation:
There is a clear opportunity for advocacy and support for the implementation of DMARC among businesses. This could be facilitated through simplified guidelines, educational content, and perhaps incentives for adoption.

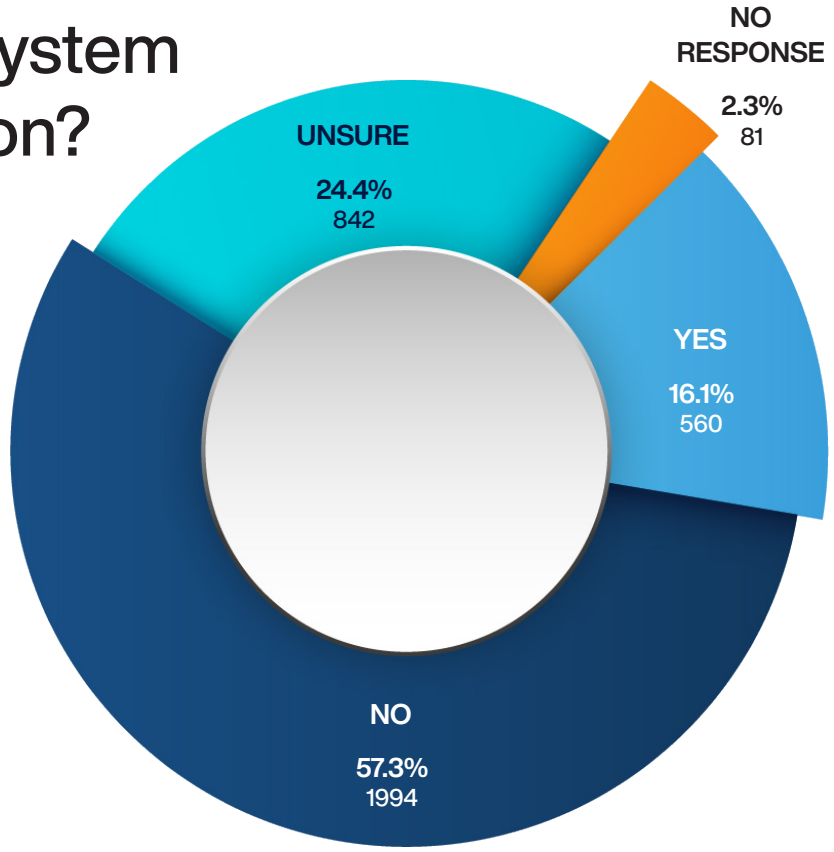
Integrating DMARC with Broader Frameworks:
Given the low levels of understanding and implementation, integrating DMARC with broader cybersecurity frameworks and ensuring it is a part of standard cybersecurity checklists could be beneficial.

Addressing Barriers to Adoption:
Identifying and addressing the barriers to DMARC adoption, such as perceived complexity or cost, should be a priority. Tailored solutions for different sizes and types of businesses could help in overcoming these barriers.

In conclusion, the data suggests a significant opportunity for improving the cybersecurity posture of businesses through the adoption of DMARC. The lack of awareness and usage of DMARC could be a contributing factor to the challenges faced with the ASD Essential 8's perceived effectiveness and maturity levels. Addressing this through targeted education and integration into cybersecurity policies could strengthen the resilience of businesses against domain spoofing and related attacks.

Question:

Do you or your IT team actively monitor system access and usage within your organisation?



Implications for Cybersecurity Strategy:

- **Risk of Unmonitored Access:** The lack of active monitoring is a significant gap in an organisation's cybersecurity strategy. Without monitoring, there is a risk that malicious activities could go undetected, increasing the potential for damage.
- **Need for Improved Cybersecurity Practices:** The data suggests a need for improved cybersecurity practices and policies that prioritise monitoring as a fundamental component of an organisation's cybersecurity defence.
- **Communication and Awareness Deficits:** The high number of respondents unsure about monitoring practices suggests that there may be a communication gap within organisations regarding cybersecurity practices and policies.

In conclusion, the data points to a notable lack of active system monitoring within a majority of the organisations represented. Given the critical role of monitoring in detecting and responding to cybersecurity incidents, the findings highlight a significant area of potential improvement for organisational cybersecurity practices. Addressing this gap is crucial for strengthening the overall cybersecurity posture of organisations.

The statistics regarding the monitoring of system access and usage within organisations indicate several points of concern for cybersecurity management:

Limited Active Monitoring:
Only a small portion of respondents (560) affirm that there is active monitoring of system access and usage by their IT team. This represents a critical aspect of cybersecurity hygiene, as active monitoring can detect unauthorized access, potential breaches, and misuse of systems.

Predominant Lack of Monitoring:
Lack of Monitoring: A significant majority of respondents (1994) indicate that their organisation does not actively monitor system access and usage. This lack of monitoring may leave these organisations vulnerable to undetected security incidents and potential data breaches.

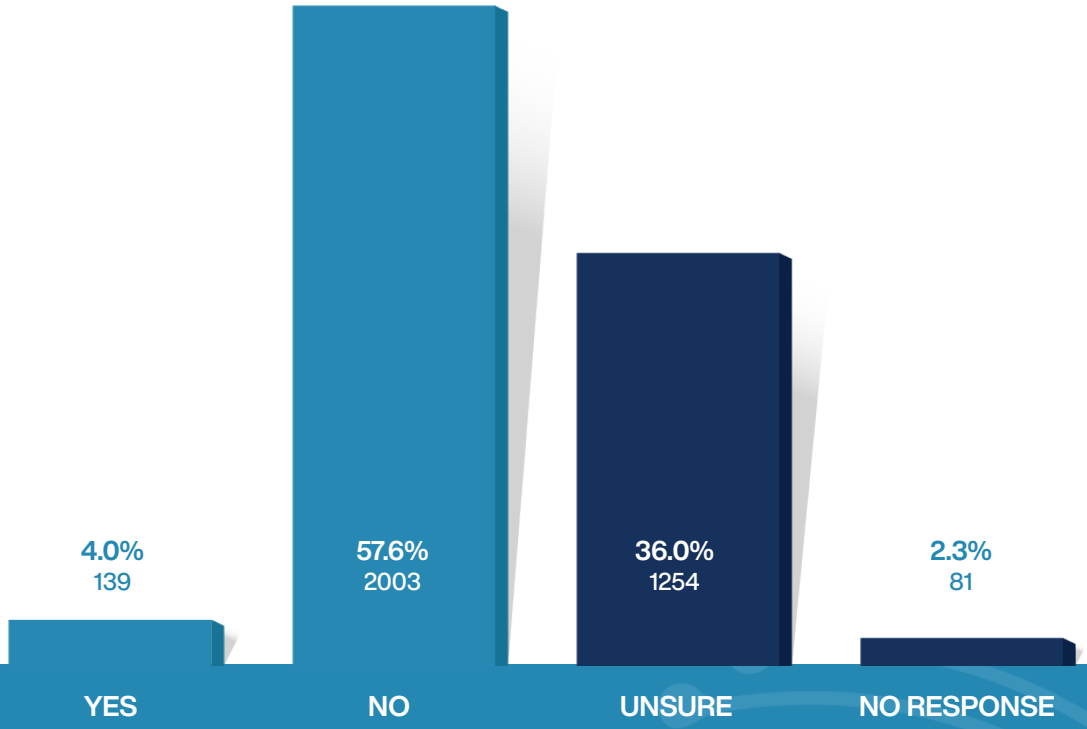
High Uncertainty:
A large number of respondents (842) are unsure whether their IT team actively monitors system access and usage. This uncertainty could reflect a lack of communication within the organisation or a deficiency in understanding of the security practices in place.

Non-Response:
There is a relatively small number of non-responses (81), which may indicate a general awareness of the question's relevance but could also represent a segment that is disengaged from cybersecurity practices.

Question:

Can your IT team detect an intruder into your Business systems in real-time?

Considering the previous data on system monitoring and DMARC usage, this paints a troubling picture of the overall cybersecurity posture across various organisations:



Correlation with Monitoring Practices:
The lack of real-time detection capabilities aligns with the previously noted deficiencies in system monitoring. Effective real-time intrusion detection often relies on having robust monitoring systems in place.

Implications for Response Times:
Without the ability to detect intrusions in real time, the response time to incidents is likely delayed, increasing the potential for damage and data loss.

Need for Enhanced Security Infrastructure:
These findings underscore the need for businesses to invest in enhanced security infrastructure, including intrusion detection systems (IDS) and security information and event management (SIEM) solutions, which are essential for real-time detection.

Training and Awareness Deficit:
The high level of uncertainty also suggests a deficit in training and awareness among staff regarding the cybersecurity capabilities of their IT infrastructure.

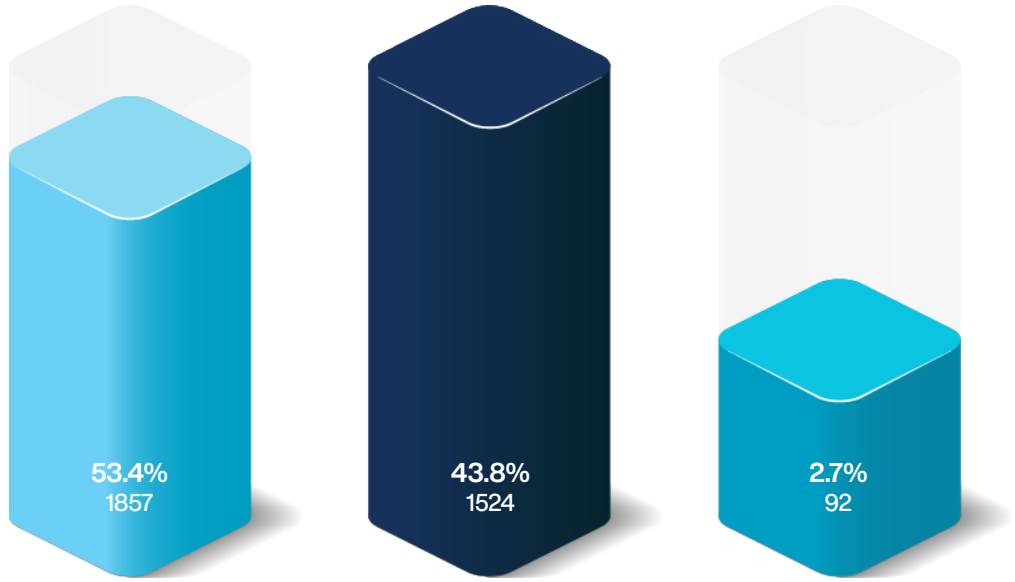
In summary, the lack of real-time intrusion detection capabilities in the majority of businesses, combined with a high degree of uncertainty about such capabilities, calls for immediate action to strengthen cybersecurity measures. This includes investing in advanced detection technologies, enhancing training and awareness programs, and ensuring that clear communication and incident response plans are in place. Addressing these issues is critical to safeguarding businesses against the increasingly sophisticated landscape of cyber threats.

THIRD PARTIES

Question:

Do you outsource your IT to a managed service provider?

The survey indicates that a majority of the respondents, 53.42%, outsource their IT to a managed service provider. This suggests a significant reliance on external expertise to manage IT needs, which could include cybersecurity management and support.



Conversely, 43.84% retain their IT operations in-house, while a small portion, 2.74%, are unsure about their IT management structure.

The trend towards outsourcing IT to specialized providers can be seen as a strategic move, particularly for small to medium-sized businesses that may not have the resources to maintain a full-fledged IT department. Managed service providers often bring a level of expertise and efficiency that can be cost-prohibitive for individual organisations to develop internally. They can also offer scalability and access to advanced technologies and methodologies, including cybersecurity services, which are crucial in the current digital landscape.

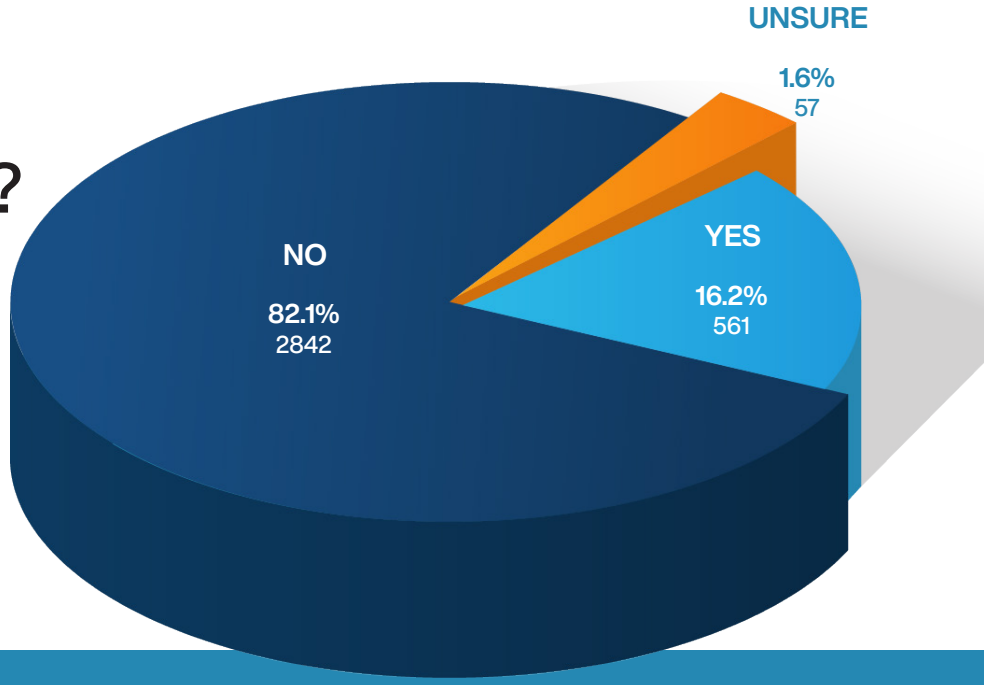
However, this reliance on external IT services also raises important considerations regarding the oversight and governance of cybersecurity practices. Organisations must ensure that their managed service providers have robust cybersecurity measures and that there is clear communication regarding the division of responsibilities for protecting against and responding to cyber incidents.

For the segment of organisations not outsourcing their IT, it is essential to recognize the importance of developing strong internal capabilities, particularly in cybersecurity, which is increasingly becoming a non-negotiable aspect of doing business in the digital age. The small percentage of respondents unsure about their IT management approach points to a potential area for improvement in terms of strategic IT planning and policy development.

The survey data underscores the diverse approaches to IT management and the prominent role of managed service providers in the contemporary cybersecurity ecosystem. Regardless of the approach taken, the data highlights the universal importance of prioritizing cybersecurity within the IT management strategy, whether it is outsourced or managed internally.

Question:

Have you seen or reviewed the cyber security capabilities of your IT provider?



The data presents a concerning picture: only 16.21% of respondents have seen or reviewed the cybersecurity capabilities of their IT provider. This leaves a vast majority, 82.14%, who have not, with a small percentage, 1.65%, unsure about whether they have undertaken such a review.

This finding is particularly striking in the context of the earlier statistic that a majority of organisations outsource their IT to managed service providers. The lack of oversight revealed by these numbers suggests a disconnect between the reliance on external IT services and the due diligence conducted by organisations on the cybersecurity prowess of these providers.

The importance of vetting an IT provider's cybersecurity capabilities cannot be overstated. Given the increasing sophistication of cyber threats and the critical role of IT service providers in managing and protecting organisational data, it is imperative for organisations to actively engage in assessing the security measures implemented by their providers.

The low percentage of organisations that have reviewed their IT provider's cybersecurity capabilities could indicate a lack of awareness of the potential risks involved or a gap in the cybersecurity governance processes within these organisations.

It may also reflect an over-reliance on the perceived expertise of IT providers without sufficient verification.

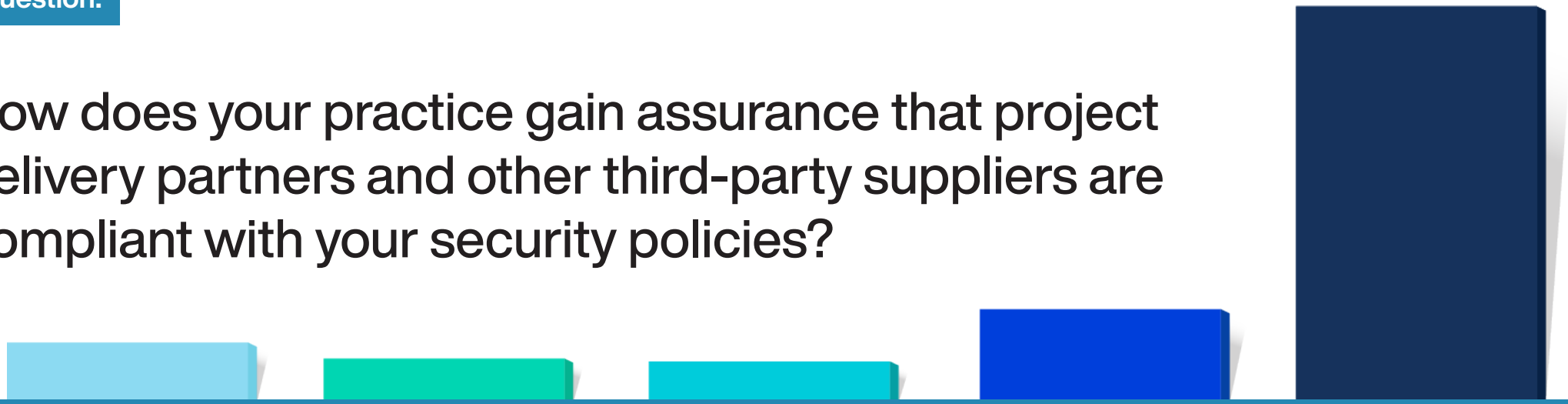
For the organisations that have not conducted such a review, there is an urgent need to establish processes for regular and thorough evaluations of their IT providers' cybersecurity measures. This should be an integral part of the contractual relationship with the provider and include clear communication about expectations, responsibilities, and the right to audit.

The survey data highlights a critical oversight in the cybersecurity practices of a significant number of organisations. It underscores the necessity for a proactive and informed approach to managing third-party IT services, especially in areas as crucial as cybersecurity. Organisations must take steps to ensure that their IT providers are not only capable of delivering services but are also equipped to protect against cyber threats, thereby safeguarding both their own and their clients' data.

tThe results revealed that 21.25% (748) of respondents know their data is stored in Australia, 4.83% (170) know it is stored overseas, and a significant 73.92% (2602) are unsure of where their data is stored. In light of these findings, this analysis aims to discuss the implications of these statistics on the overall cybersecurity posture of these organisations and the potential legal consequences of storing data offshore.

Question:

How does your practice gain assurance that project delivery partners and other third-party suppliers are compliant with your security policies?



9.3% | 323

Information security requirements are detailed in contracts.

7.6% | 262

Your right to audit is detailed in contracts and is exercised.

7.5% | 187

The need to meet recognised standards (such as ISO27001:2013) is stipulated.

14.5% | 136

The practice's compliance is measured through self-assessment.

61.0% | 502

We do not do third party supplier cyber reviews

The survey unveils a critical perspective on how organisations assure compliance with security policies among project delivery partners and third-party suppliers.

A mere 9.33% of respondents have information security requirements detailed in contracts, and only 7.57% have contractual audit rights that are actively exercised. Slightly more, 7.54%, require adherence to recognized standards such as ISO27001:2013. Interestingly, 14.50% rely on self-assessment measures for compliance. However, the majority, 61.05%, admit to not conducting cyber reviews of third-party suppliers at all.

This data paints a concerning picture of the cybersecurity oversight landscape. The low percentages of organisations that have taken proactive contractual steps or engaged in audit practices suggest a broader trend of insufficient diligence regarding third-party cybersecurity risks. The reliance on self-assessment for compliance measurement, while useful, may not provide the rigorous validation needed to ensure that external parties' security practices align with an organisation's standards.

The most startling revelation, however, is that the significant majority do not conduct third-party supplier cyber reviews. This oversight represents a substantial gap in cybersecurity defenses, given that third-party suppliers can be a common vector for security breaches. In an interconnected digital ecosystem, the security posture of third-party partners is as crucial as that of the contracting organisation itself.

The survey underscores the need for a systematic approach to third-party cybersecurity management, including the establishment of clear contractual requirements, regular audits, and adherence to recognized standards. The data also indicates a potential need for industry-wide frameworks and guidelines that could support organisations in implementing robust third-party cybersecurity assessment practices.

The survey results highlight a critical area of cybersecurity that requires immediate attention and action. Ensuring the security compliance of third-party suppliers is not just a best practice but a necessity in an era where organisational boundaries are increasingly porous, and security is only as strong as the weakest link in the supply chain.

Question:

Does your organisation measure the effectiveness of cybersecurity implementations and actions across your business?

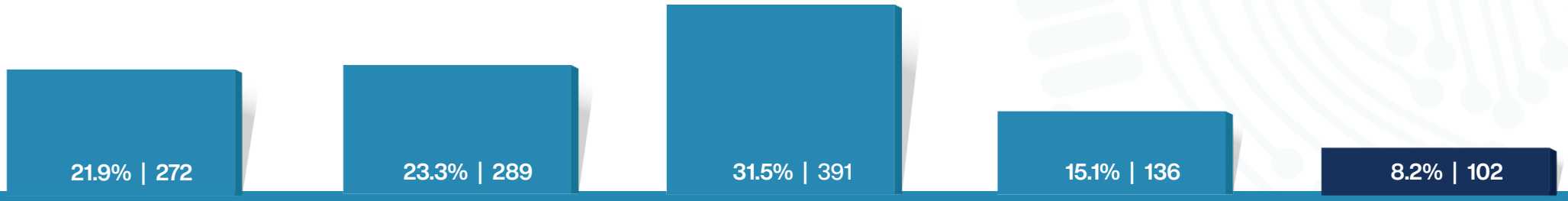
From the 2023 State of Cyber Security Survey, it is evident that organisations vary in their approach to measuring the effectiveness of cybersecurity implementations.

A proactive segment (21.92%) seriously monitors cybersecurity threats in alignment with internal business requirements and investments, while a slightly larger group (23.29%) not only monitors but also actively adjusts their business requirements based on the evolving threat landscape.

However, a significant portion of respondents (31.51%) monitor their systems without measuring effectiveness, which could indicate a lack of comprehensive cybersecurity strategy or a gap in their ability to evaluate their defensive measures. Furthermore, 15.07% of organisations do not monitor the effectiveness of their cybersecurity at all, suggesting a notable area of vulnerability. The 8.22% who have no idea about their monitoring status highlight a concerning lack of awareness or engagement with cybersecurity practices.

When considering the earlier survey responses, which reflect various levels of cybersecurity maturity and preparedness, these figures suggest that while some organisations are making concerted efforts to ensure their cybersecurity measures are effective, there is still a substantial number of businesses that need to develop or improve their monitoring and evaluation processes.

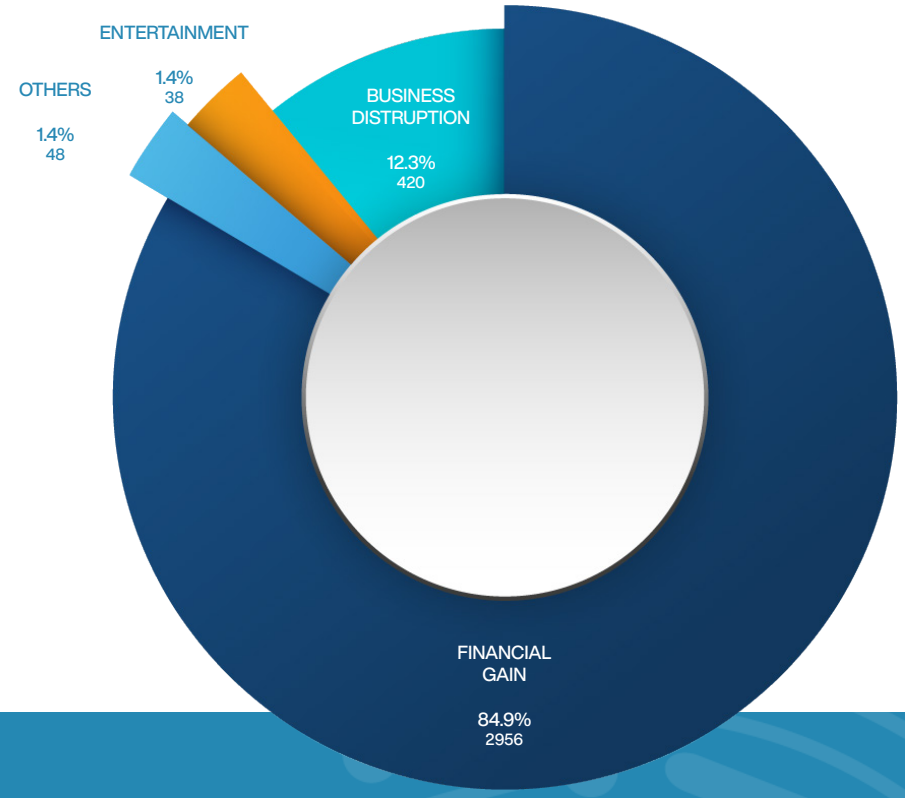
The data underscores the importance of not only implementing cybersecurity solutions but also continuously assessing and refining these measures to ensure they remain effective against an ever-changing threat landscape. It also points to the necessity for better education and communication regarding the importance of monitoring and evaluation in the field of cybersecurity.



INCIDENTS

Question:

What do you believe is the primary focus of cyber-attacks?



The 2024 State of Cyber Security Survey indicates an overwhelming consensus among respondents that financial gain is the primary motivator behind cyber attacks, with 84.93% aligning with this perspective.

This is followed by a smaller fraction, 12.33%, who consider business disruption as the main focus. Notably, reputational damage and revenge are not seen as primary drivers, as indicated by 0% of respondents for each category. Entertainment and other unspecified reasons are considered the main focus by 1.37% of respondents respectively.

This data reflects a recognition that cyber attacks are largely profit-driven, aligning with global trends where ransomware and data breaches for financial extortion are rampant. The lack of concern for reputational damage or revenge as motivators may indicate that respondents view cyber attacks more as a professional criminal enterprise rather than actions driven by personal vendettas or for the purpose of inflicting reputational harm.

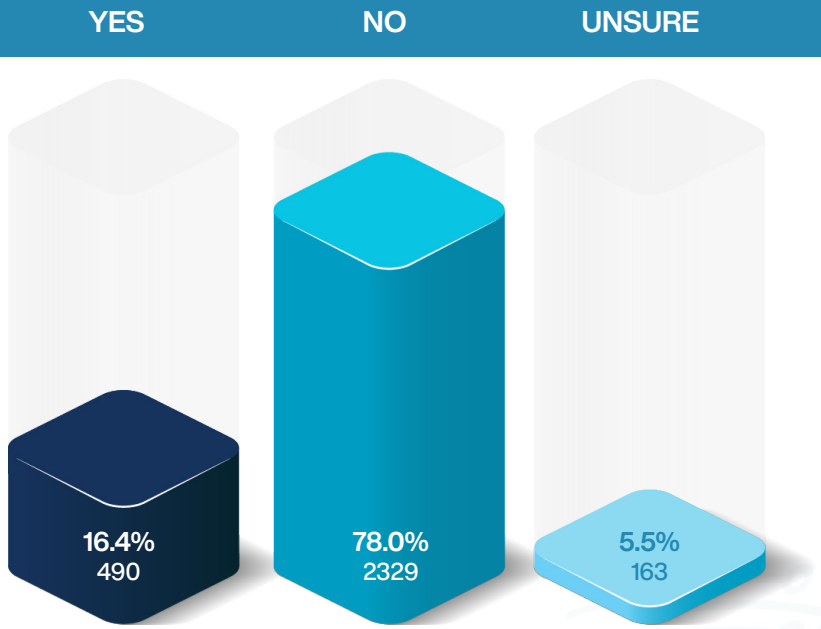
Considering the perceived lack of focus on reputational damage, it is essential to acknowledge that while it may not be the primary goal, it is often a consequential outcome of cyber attacks. Therefore, organisations should not underestimate the reputational impact when strategizing their cybersecurity measures.

The recognition of financial gain as the primary objective underscores the necessity for robust financial and data protection systems. It also stresses the importance of regular security training focused on recognizing and mitigating attacks that could lead to financial loss, such as phishing and social engineering tactics.

In summary, the survey results highlight the importance of understanding the motivations behind cyber attacks to better tailor cybersecurity defenses. It is clear that organisations need to prioritize the protection of financial assets and sensitive data, as these are the most lucrative targets for cybercriminals.

Question:

Has your organisation had a cyber incident within the past 12 months?



The survey indicates that 16.44% of organisations experienced a cyber incident within the past 12 months.

While this number represents a significant portion of businesses acknowledging the direct impact of cyber threats, a much larger majority, 78.08%, reported not having experienced an incident, and 5.48% are unsure.

The disparity between the number of organisations that have faced a cyber incident and those that have not could be influenced by several factors, including the varying levels of cybersecurity measures in place, differences in threat exposure, and possibly underreporting due to lack of detection or awareness.

The figure also raises questions about preparedness and response. Considering the previous data on the low percentage of organisations that have a cyber insurance policy or conduct regular cybersecurity training, those that reported no incidents could potentially be at risk due to a false sense of security or unrecognized vulnerabilities.

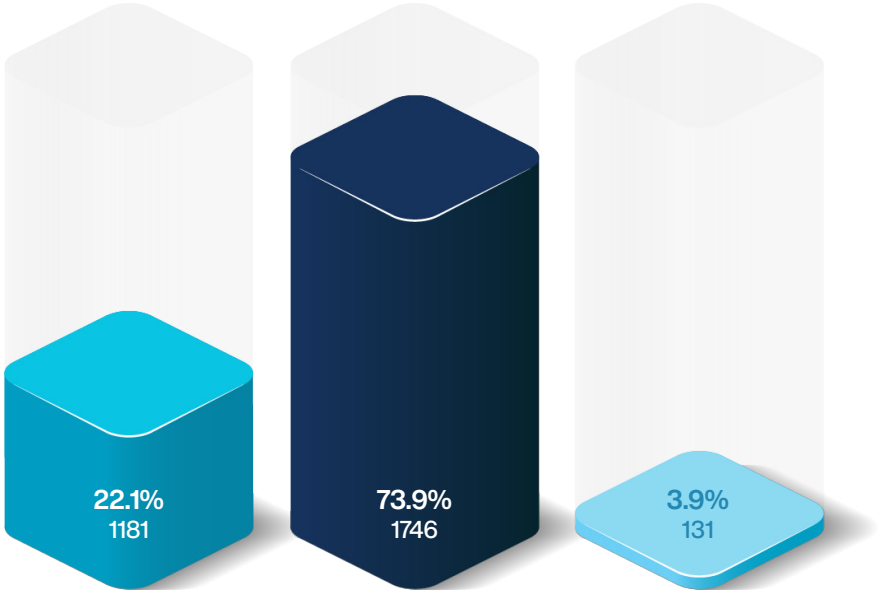
The uncertainty reported by some organisations regarding their cyber incident experience is indicative of a possible lack of adequate monitoring and incident detection mechanisms. Without proper systems to identify and track security breaches, organisations may be unaware of compromised data or ongoing malicious activities.

Taken together, these statistics underscore the importance of a proactive and comprehensive cybersecurity strategy. This includes regular training, monitoring, implementing robust security protocols, and considering cyber insurance as part of risk management practices. Understanding and acknowledging the real possibility of cyber threats are crucial steps toward strengthening defenses and mitigating potential impacts on the organisation.

Question:

Do you currently have a written cyber incident response plan?

The recent figures from the 2023 State of Cyber Security Survey cast a stark light on the readiness of industries to manage and respond to cyber incidents effectively.



A scant 22.10% of respondents have a written cyber incident response plan in place. This is a disquieting statistic, given the heightened state of cyber threats in our digital era. The majority, at 73.93%, report no such plan, and a further 3.96% remain unsure of their stance.

This data suggests a troubling gap between the need for preparedness in the face of inevitable cyber incidents and the current state of readiness across various sectors. Without a well-defined incident response plan, organisations find themselves at a disadvantage, unable to respond swiftly or effectively to mitigate the consequences of cyberattacks.

The lack of a formalized plan could be symptomatic of several underlying issues: a possible lack of awareness about the risks, a deficit in cybersecurity literacy, or even the daunting prospect of developing such a plan from scratch. For small and medium-sized businesses, the challenges are often magnified by limited budgets and expertise. However, this does not diminish the necessity of such a plan; if anything, it underscores the importance of accessible resources and support for these businesses to bolster their cyber defenses.

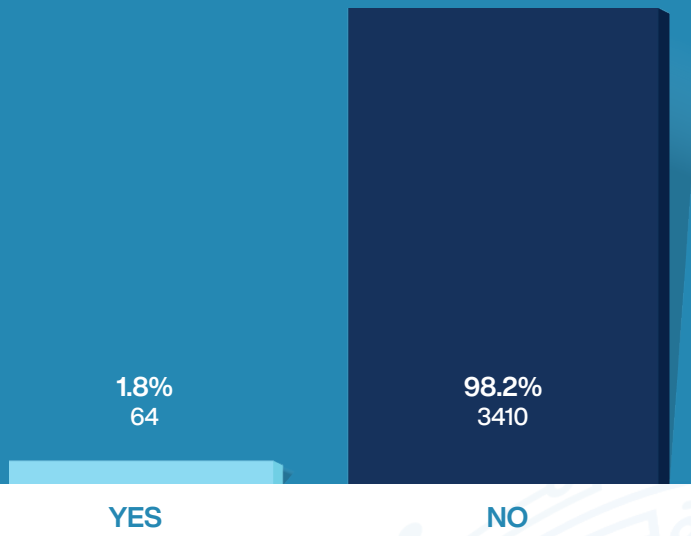
Larger organisations, despite having more resources, seem to also struggle with instituting a comprehensive cyber incident response plan. This may be due to the complex and layered nature of their IT environments, which can make the development of a plan a more intricate task. Nonetheless, the imperative to have a tailored response strategy that can be rapidly deployed in the event of an incident is clear.

The survey's findings should serve as a clarion call to all sectors that cybersecurity requires urgent and sustained attention. It is essential for organisations to recognize that an incident response plan is not merely a regulatory checkbox or an IT department concern; it is a fundamental component of a robust risk management strategy and a reflection of an organisation's resilience.

In light of these statistics, it is incumbent upon all organisations, regardless of size, to prioritize the development of a cyber incident response plan. Such a plan should not only be written but also regularly updated, tested, and ingrained within the organisational culture. Moreover, industry leaders and regulatory bodies must work together to provide frameworks, tools, and education to support all organisations in this critical endeavor.

Question:

Have you fully tested your cyber incident response plan with an external organisation?



The survey responses here highlight a critical shortfall in cybersecurity readiness across surveyed industries. When considering that only 22.10% of respondents have a written cyber incident response plan, the additional data point that a mere 1.84% have fully tested their plans with an external organisation is even more alarming.

This starkly low percentage of external testing indicates a significant vulnerability in the practical readiness of organisations to manage cyber incidents. The process of testing an incident response plan with an external entity is not merely a step towards validation, but also a crucial exercise in identifying weaknesses and improving response capabilities. It provides an objective assessment of how an organisation's plan stands up to scrutiny and can adapt to the evolving tactics of cyber adversaries.

Given the scant number of organisations that have a written plan in the first place, it follows that even fewer would have reached the stage of full external testing. This gap points to a widespread trend of underpreparedness that transcends sectors and sizes of businesses. It suggests that, while some organisations may recognize the theoretical importance of incident response planning, the practical application and validation of these plans are not being prioritized.

The lack of external testing could be attributed to several factors. For many organisations, particularly SMBs, the resources and expertise required to conduct such testing may be lacking. There may also be a degree of complacency, with some organisations perhaps overestimating the efficacy of their in-house testing or underestimating the complexity of real-world cyberattacks. For larger entities, the challenge may lie in the coordination of complex and distributed systems, making comprehensive testing a significant undertaking.

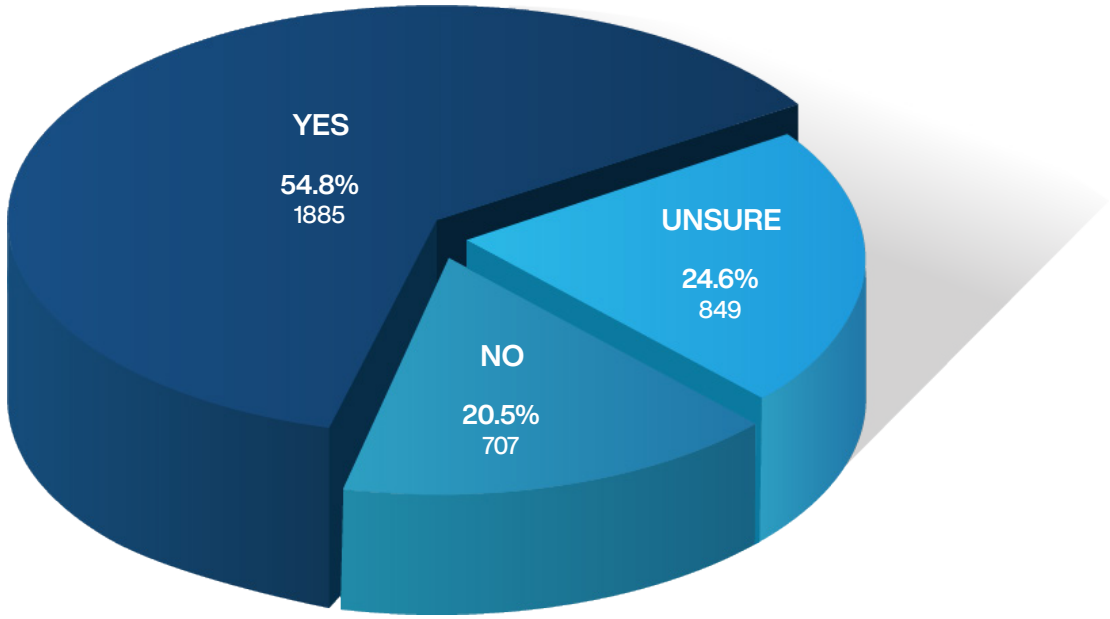
However, the benefits of external testing are clear. It can uncover blind spots that internal teams may overlook and provide valuable insights into an organisation's incident response efficacy from an attacker's perspective. It also prepares teams for the stress and unpredictability of an actual cyber incident, which cannot be fully replicated by internal exercises alone.

The survey data serves as a clarion call for industries to not only establish and document cyber incident response plans but also to ensure these plans are robustly tested and verified. This may involve leveraging partnerships for cybersecurity expertise, investing in regular external audits and simulations, and cultivating a culture that values and understands the critical role of cybersecurity in maintaining operational integrity.

In essence, the path to resilience in cyber incident management is a continual process that requires both the creation of comprehensive plans and the rigorous testing of these plans against real-world scenarios. As cyber threats continue to escalate in sophistication and impact, the necessity for such preparedness has never been more imperative.

Question:

Does your organisation have the skills needed to respond to and recover from a cyberattack?



The information collected reveals a landscape of self-assessed cyber resilience capabilities among organisations, with 54.79% feeling they possess the necessary skills to respond to and recover from a cyberattack. This sense of readiness is encouraging, especially in light of the statistics indicating varying degrees of preparedness in other areas, such as the implementation of risk management strategies and the monitoring of password reuse.

However, 20.55% of respondents do not believe they have the skills needed for an effective cyber response, and a significant 24.66% are unsure of their capabilities. This uncertainty may reflect the complexities of cyber threat management and the dynamic nature of the threat landscape, which demands continuously updated skills and knowledge.

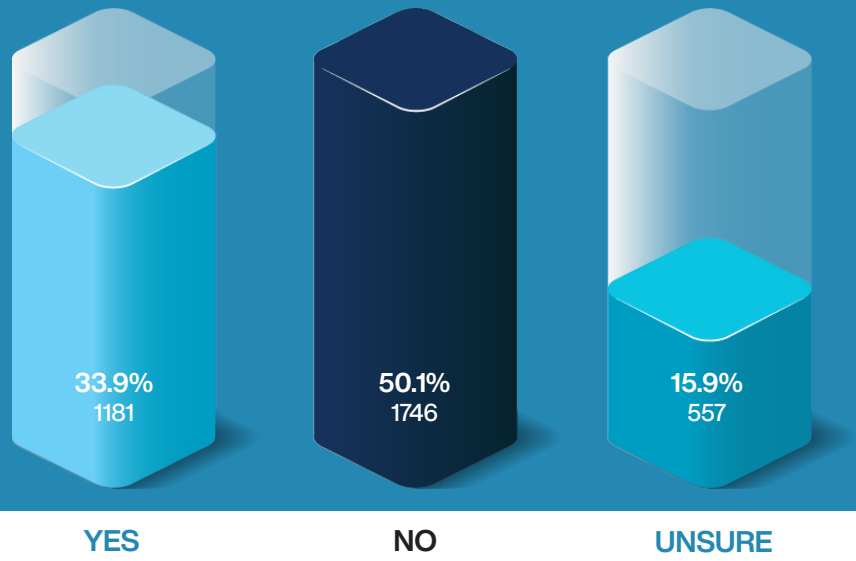
The data suggests that while over half of the organisations are confident in their cybersecurity skills, there remains a substantial proportion that either acknowledges a skills gap or is uncertain about their level of preparedness. This gap is concerning, given the high rates of password reuse and the low engagement in third-party cybersecurity audits and cyber insurance policies reported in the survey.

The presence of a skills gap or uncertainty in nearly half of the surveyed organisations underscores the importance of ongoing training and education in cybersecurity. This is reinforced by the earlier data indicating that a significant number of organisations have conducted cybersecurity awareness training in the last six months and engage in regular training sessions. Yet, the reported confidence levels suggest that training frequency and content may not be sufficiently comprehensive or that the effectiveness of these training initiatives could be improved.

In conclusion, the survey indicates a need for a strategic approach to developing cybersecurity skills across all organisations. This includes regular, up-to-date training, clearer communication about cybersecurity measures and expectations, and a thorough review of current cybersecurity practices to address any gaps in skills or knowledge. As the cyber threat landscape continues to evolve, so too must the capabilities of organisations to respond and recover effectively.

Question:

Does your organisation have a fully written disaster recovery plan?



The findings on disaster recovery plan adoption among Australian organisations underscore the importance of having a comprehensive, fully written plan in place.

Businesses should prioritize the development and regular review of a disaster recovery plan to ensure they are prepared to respond to and recover from potential incidents effectively. Additionally, organisations should focus on improving communication, training, and oversight related to disaster recovery planning to ensure all employees understand their roles and responsibilities in the event of a disruption.

The results revealed the following distribution: 33.90% (1181) have a fully written disaster recovery plan, 50.11% (1746) do not, and 15.99% (557) are unsure. This analysis aims to discuss the implications of these statistics on the overall cybersecurity posture of these organisations and the importance of having a disaster recovery plan in place.

Organisations with disaster recovery plans

The 33.90% of organisations with a fully written disaster recovery plan demonstrate a proactive approach to managing potential cyber threats and system failures. These businesses are better prepared to respond to and recover from incidents, minimizing downtime and associated costs.

Lack of disaster recovery plans

The 50.11% of organisations without a disaster recovery plan expose themselves to significant risks in the event of a cyber attack, natural disaster, or other disruptive events. These businesses may face extended downtime, financial losses, reputational damage, and potential legal consequences if they cannot quickly and effectively respond to and recover from an incident.

Uncertainty about disaster recovery plans

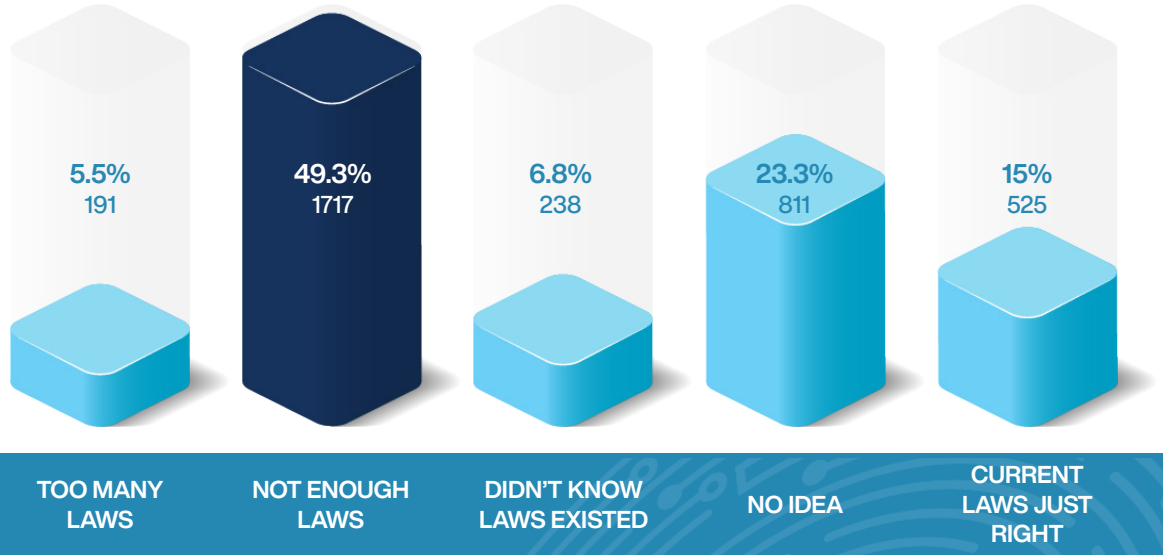
The 15.99% of organisations that are unsure whether they have a disaster recovery plan highlights a concerning lack of awareness about their organisation's preparedness for disruptive events. This lack of knowledge may indicate insufficient communication, training, or oversight related to disaster recovery planning within these organisations.


GOVERNMENT

Question:

Do you believe Cyber security laws and regulations are sufficient?

The 2023 State of Cyber Security Survey results reveal a significant sentiment among respondents regarding the adequacy of cybersecurity laws and regulations.



Nearly half, at 49.3%, feel that there are not enough laws governing cybersecurity. A smaller but substantial percentage, 23.3%, are uncertain about the sufficiency of existing laws, and 6.9% were not even aware that such laws existed. Only a minority, 15.1%, believe that the current laws are just right, while 5.5% think there are too many laws.

This distribution of opinions indicates a general consensus that current cybersecurity legislation may be lagging behind the rapidly evolving cyber threat landscape. The lack of awareness and uncertainty about cybersecurity laws could be indicative of a communication gap between lawmakers, regulators, and the general public, as well as within organisations themselves.

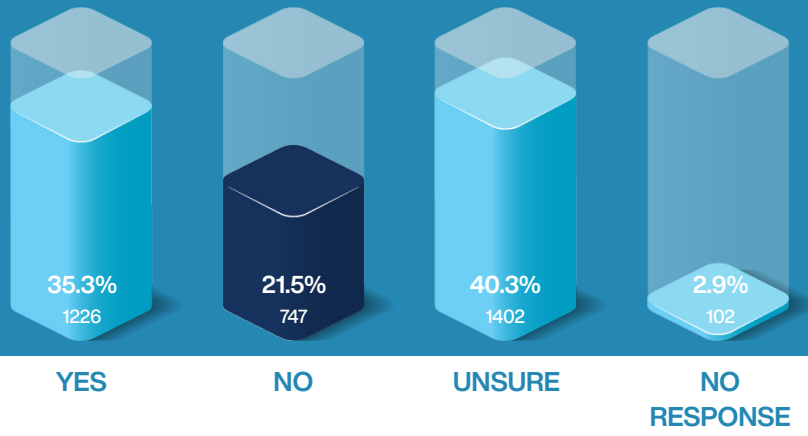
The relatively low percentage of respondents who think the current laws are just right suggests that while some are satisfied, there may be room for improvement in terms of the scope, enforcement, or effectiveness of these laws. On the other hand, the small proportion who believe there are too many laws might reflect concerns about overregulation potentially hindering business operations or innovation.

These perspectives emphasize the need for ongoing dialogue between policymakers, cybersecurity professionals, industry stakeholders, and the public to ensure that cybersecurity laws are comprehensive, clear, and agile enough to adapt to new challenges.

In summary, the survey highlights the need for a critical evaluation of current cybersecurity laws and regulations, considering the perceived insufficiency and the gaps in awareness among those affected by them. It also points to the necessity for proactive measures to address these challenges, ensuring that laws are not only sufficient but also well-communicated and understood by all stakeholders.

Question:

Do you understand your legal obligations for Cyber Security and Privacy in Australia?



The statistics regarding the understanding of legal obligations for cybersecurity and privacy in Australia among respondents reflect varying levels of awareness.

Partial Understanding: Just over a third of the respondents (35.26%) affirm that they understand their legal obligations for cybersecurity and privacy. This level of understanding is fundamental for compliance and suggests that these respondents may have implemented necessary measures to adhere to these obligations.

Significant Lack of Awareness: More than one-fifth (21.48%) of respondents do not understand their legal obligations, which raises concerns about potential non-compliance risks. This lack of understanding can leave businesses vulnerable to legal repercussions, including fines and reputational damage.

High Uncertainty: The largest group of respondents (40.32%) are unsure about their legal obligations, indicating a significant gap in legal awareness. This uncertainty can lead to inconsistent application of cybersecurity and privacy measures and poses a risk to the organisations' adherence to legal standards.

Non-Response Rate: A small percentage (2.93%) did not respond, which could be attributed to a variety of factors, such as indifference, lack of knowledge, or the perception that the question is not applicable to them.

Implications and Considerations:

Need for Legal and Compliance Education: The data suggests a strong need for education on the legal aspects of cybersecurity and privacy, as a lack of understanding can impede the effective management of cyber risks.

Potential Compliance Risk: With a high percentage of respondents either not understanding or being unsure about their legal obligations, there is a potential risk for non-compliance, which could have serious legal and financial implications.

Integration of Legal Obligations in Cybersecurity Strategy: The findings highlight the importance of integrating legal obligations into the overall cybersecurity strategy of an organisation. This includes not only technical measures but also legal compliance and data protection practices.

Role of Industry and Government: The statistics may prompt industry bodies and the government to take further action in providing resources and guidance to help organisations understand and meet their legal obligations.

Recommendations for Addressing the Issues:

Focused Training on Cyber Law: Organisations should consider providing focused training on the legal aspects of cybersecurity to ensure that all relevant personnel are aware of their obligations.

Regular Legal Updates: Businesses should stay informed of any changes in cybersecurity and privacy laws and regulations through regular updates and legal advisories.

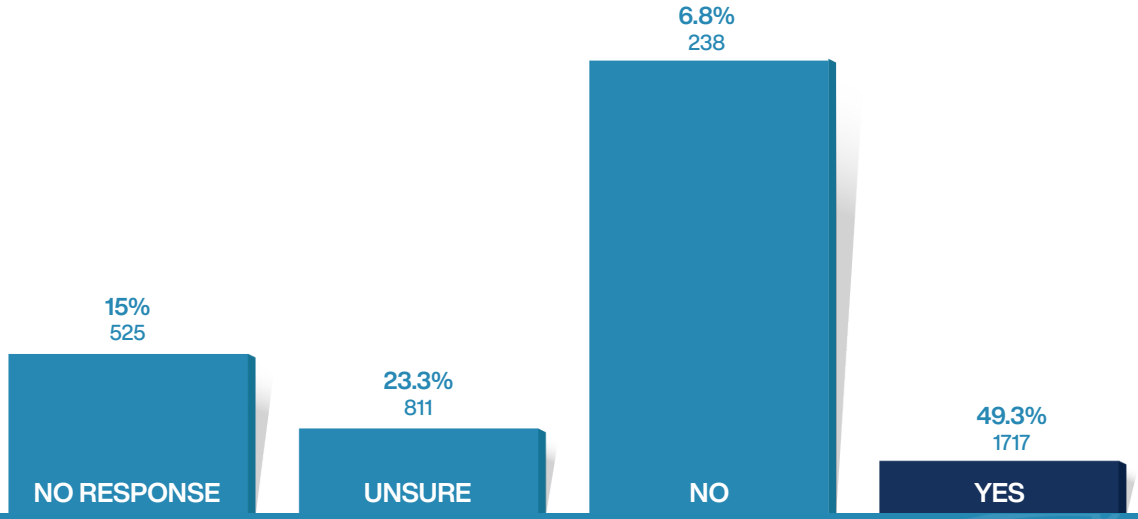
Legal Compliance Audits: Regular compliance audits can help organisations assess their adherence to legal obligations and identify areas for improvement.

Consultation with Legal Experts: Engaging with legal experts specialised in cybersecurity and data protection laws can help organisations navigate the complexities of compliance.

In conclusion, the statistics indicate a notable need for improvement in the understanding of legal obligations related to cybersecurity and privacy in Australia. Addressing this knowledge gap is crucial for businesses to effectively manage their cyber risks and ensure compliance with Australian laws and regulations.

Question:

Do you understand the ASD Essential 8?



Low Level of Understanding: A mere 9.15% of respondents affirm that they understand the ASD Essential 8. This low percentage is a critical finding, as it suggests that the vast majority of respondents may not have a clear grasp of what the Essential 8 entails, which is a fundamental prerequisite for effective implementation and perception of its benefits.

High Level of Non-Understanding: An overwhelming majority of 73.91% indicate they do not understand the Essential 8. This lack of understanding is a significant barrier to effective cybersecurity practices. It suggests that the Essential 8 either has not been communicated effectively to these individuals or that it is not accessible or relatable enough for them to comprehend.

Considerable Uncertainty: Additionally, 13.59% of respondents are uncertain about their understanding of the Essential 8. This further underscores the issue of clarity and accessibility of information regarding the framework.

Consistent Non-Response Rate: The non-response rate is consistent at 3.34% across the various questions posed, indicating a consistent segment that is either disengaged or lacks sufficient information to provide a response.

In-depth commentary considering these findings:

Impact on Cybersecurity Posture: The data strongly suggests that the understanding of the ASD Essential 8 is limited among respondents. This lack of understanding is likely contributing to the previously noted uncertainty and skepticism about the framework's effectiveness. Without a solid understanding of the Essential 8, organisations cannot fully implement its strategies, thus potentially compromising their cybersecurity posture.

Need for Enhanced Communication and Training: These findings highlight an urgent need for enhanced communication, education, and training regarding the ASD Essential 8. Cybersecurity frameworks must be understood to be effective, and this education should be accessible to all levels within an organisation, not just IT professionals.

Correlation with Reporting and Effectiveness: The lack of understanding could also correlate with the low reporting rates of phishing emails. If respondents do not understand the Essential 8, they may not be aware of the importance of reporting as a critical element of a comprehensive cybersecurity strategy.

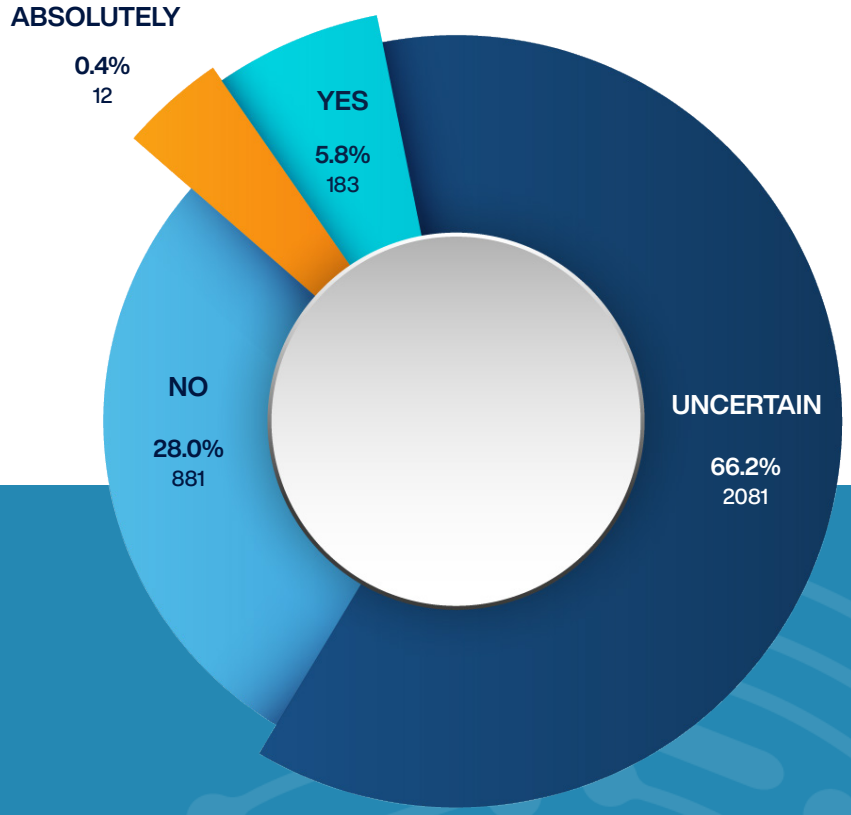
Influence on Cybersecurity Strategy Development: This gap in understanding can influence how organisations develop and adapt their cybersecurity strategies. If the Essential 8 is not well understood, organisations may fail to see the need to progress to higher maturity levels within the framework, which could stifle the development of more robust cybersecurity defenses.

Conclusions for Research:

Understanding the ASD Essential 8 is a critical factor that seems to be missing for a large portion of respondents. This gap likely impacts both the implementation of the Essential 8 and the perception of its effectiveness. Your research could delve into strategies for improving the understanding of cybersecurity frameworks like the Essential 8, perhaps by recommending that such frameworks be accompanied by comprehensive, clear, and ongoing educational initiatives. These initiatives could help bridge the gap between cybersecurity knowledge and practice, ultimately leading to more resilient organisations.

Question:

Do you believe the ASD Essential 8 works for your business?



The data provided reflects the perceptions of various businesses regarding the effectiveness of the ASD Essential 8 cybersecurity framework for their operations.

Key observations from the data include:

Minimal Strong Affirmation:
A very small fraction of the respondents, only 0.38%, firmly believe that the ASD Essential 8 is absolutely effective for their business. This negligible percentage suggests that there may be a lack of strong conviction or visible results among most businesses regarding the framework's effectiveness.

Modest Agreement:
A slightly higher, yet still modest, 5.82% of respondents agree that the Essential 8 works for their business. This reinforces the notion that while there is some level of acknowledgment of the framework's benefits, it is not overwhelmingly recognised as effective across the board.

Significant Uncertainty:
The majority of respondents, 66.17%, are uncertain about the effectiveness of the ASD Essential 8 for their business. This overwhelming majority could indicate several things, such as a lack of understanding of the framework, an inability to properly implement it, or a failure to see tangible benefits from its application.

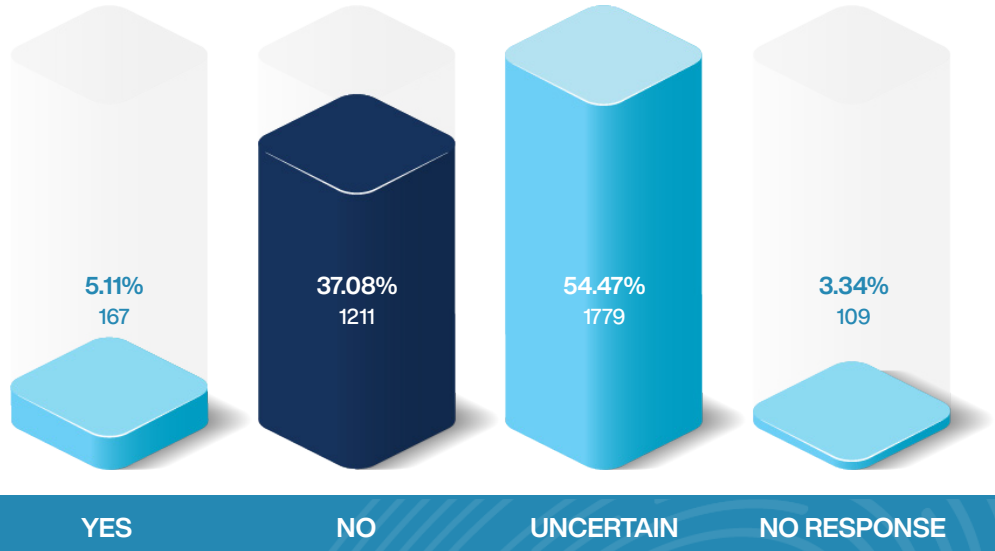
Substantial Disagreement:
A notable 28.01% of businesses do not believe that the Essential 8 is effective for their business. This significant percentage could be due to various reasons, including possible challenges in implementation, incompatibility with business processes, or perceived insufficiency in mitigating cyber threats.

Non-Response:
There is a 3.47% non-response rate, which may suggest a lack of engagement or interest in the topic, or it could reflect respondents who are not informed enough about the Essential 8 to have an opinion."

Question:

Do you believe the ASD Essential 8 is effective in preventing Cyber Attacks?

The data indicates varied levels of confidence in the ASD Essential 8's effectiveness in preventing cyber attacks among respondents. A comprehensive analysis, considering the previous statistics on its application and perceptions of its suitability for businesses, reveals significant insights.



Key observations from the data include:

Low Affirmative Rate:
Only a small percentage (5.11%) affirm that the ASD Essential 8 is effective in preventing cyber attacks. This figure is considerably low and suggests that there may be a lack of tangible evidence of effectiveness or a lack of understanding of the framework's impact among the respondents.

High Level of Skepticism:
The data shows a relatively high percentage (37.08%) of respondents do not believe in the effectiveness of the ASD Essential 8. This skepticism could stem from a variety of factors, such as personal or industry-wide experiences of cyber incidents despite the implementation of the Essential 8, or possibly a belief in the necessity for more comprehensive or different security measures.

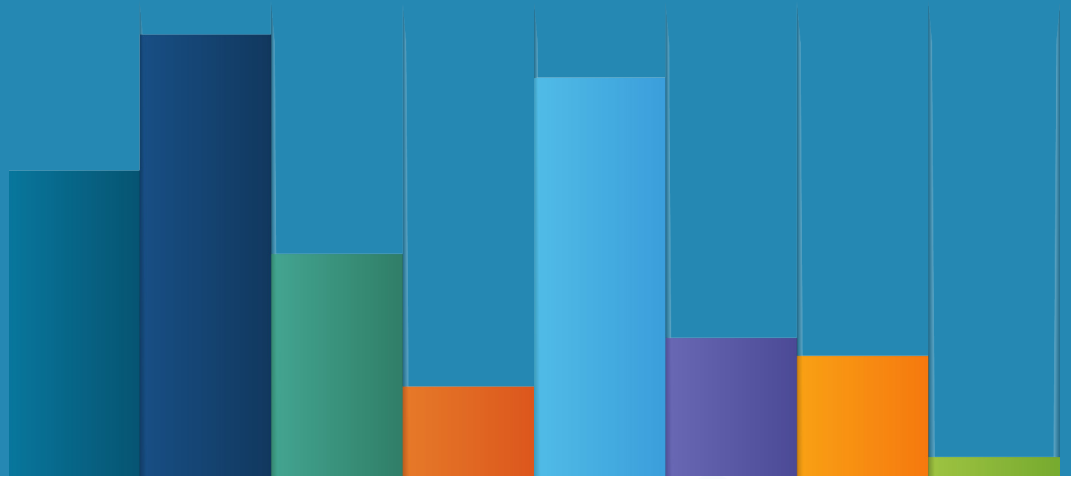
Predominant Uncertainty:
Over half of the respondents (54.47%) are uncertain about the framework's effectiveness. This prevailing uncertainty could correlate with the previously noted uncertainty about whether the Essential 8 works for their business. It may reflect challenges in the successful implementation of the framework, variations in cyber threat landscapes, or an insufficient communication of the framework's benefits and successes.

Non-Response Consideration:
The non-response rate (3.34%) remains consistent with the previous statistic, suggesting a segment of the audience remains disengaged or uninformed about the Essential 8."

Question:

What are the biggest challenges with the ASD Essential 8?

The provided statistics from 3,266 respondents outline significant challenges perceived with the ASD Essential 8 cybersecurity framework, which could offer explanations for the previous data on understanding and perceived effectiveness.



(MULTIPLE CHOICE QUESTION)

73.9%	92.5%	48.0%	19.1%	82.8%	28.2%	25.9%	4.7%
2415	3022	1569	623	2703	921	847	154

Key observations from the data include:

Comprehensiveness Concerns: A large majority, 73.94%, feel that the ASD Essential 8 does not cover all aspects of cybersecurity. This perception could lead to a lack of confidence in the framework's ability to provide a complete security solution.

Complexity and Accessibility: The most striking statistic is that 92.53% of respondents find the Essential 8 too difficult to read and understand, suggesting that the technical complexity is a significant barrier to adoption, particularly for business owners who may not have specialized knowledge.

Implementation Cost: Nearly half of the respondents, 48.04%, cite the expense of implementation as a major challenge. This highlights a financial barrier that could prevent businesses, especially small and medium-sized enterprises (SMEs), from adopting the framework.

Cloud Security: There is a concern among 19.08% of respondents that the Essential 8 does not effectively cover cloud computing, which is an increasingly critical component of modern business operations.

Maturity Level Achievement: A significant 82.76% of individuals believe it is impossible for businesses to achieve the appropriate maturity levels as prescribed by the Essential 8. This could indicate that the steps to reach higher maturity levels are not well communicated or are perceived as unattainable.

Risk and Governance: Concerns about risk management and governance are noted by 28.20% and 25.93% of respondents, respectively, suggesting that these critical areas may need more emphasis within the framework.

Other Challenges: A smaller segment, 4.72%, have other unspecified challenges with the Essential 8.
In-depth commentary considering these findings:

Barrier to Effective Cybersecurity: The complexity of the Essential 8 is a significant barrier to effective cybersecurity. If business owners cannot understand the guidelines, they cannot implement them, which may contribute to the low levels of reporting and the widespread uncertainty about the framework's effectiveness.

Financial Constraints: The cost of implementation being prohibitive for nearly half the respondents highlights a need for more cost-effective cybersecurity solutions, particularly tailored for SMEs.

Emerging Technologies: The concern that the Essential 8 does not adequately cover cloud computing is notable in an era where businesses are increasingly reliant on cloud services. This suggests a gap between the framework and the evolving technological landscape.

Realistic Goals and Communication: The belief that achieving appropriate maturity levels is nearly impossible suggests that either the goals set by the Essential 8 are unrealistic or that there is a significant communication gap. It is crucial for cybersecurity frameworks to set achievable, clear goals and provide guidance on how to reach them.

Holistic Approach: The Essential 8 may need to evolve to more holistically address risk management and governance to meet the needs of a broader range of businesses.

Conclusions for Research:

The challenges outlined by respondents suggest a disconnect between the Essential 8 framework and the practical realities of businesses, especially in terms of comprehensiveness, complexity, cost, and relevance to emerging technologies.

For your research, it would be pertinent to discuss these challenges in detail, exploring how they can be addressed to improve the framework's accessibility, applicability, and perceived effectiveness. This could involve simplifying the language, providing more resources and support for implementation, adjusting the framework to better cover cloud environments, and ensuring that the goals for achieving maturity levels are both realistic and attainable.

Maturity Results for ASD Essential 8 across 224 Audits and 5 different industries

The Australian Signals Directorate (ASD) Essential Eight Maturity Model offers a way to assess and score the cybersecurity posture of an organisation by measuring the implementation of eight essential mitigation strategies.

Each of these strategies can be scored at one of three distinct maturity levels, which reflect the depth and robustness of their implementation. Here's a detailed look at each maturity level:

Maturity Level One

- **Basic Implementation:** The organisation has taken initial steps to implement the Essential Eight strategies, but these are not comprehensive. Measures might be applied inconsistently across the organisation and may not cover all systems.
- **Ad Hoc Measures:** There is an ad hoc or partial implementation of security controls, which might offer limited protection against less sophisticated threat actors.
- **Minimal Coverage:** The security measures in place do not cover all potential threat scenarios and are more reactive than proactive.

Maturity Level Two

- **Good Practice:** The organisation has fully implemented all the Essential Eight mitigation strategies to the extent described by the ASD.
- **Consistent Application:** Security measures are applied consistently across the organisation, and there is a structured approach to cybersecurity.
- **Increased Protection:** The organisation is now more secure against a wider array of threats, including more sophisticated attacks, but may still be vulnerable to advanced adversaries.

Maturity Level Three

- **Tailored Implementation:** The organisation has not only implemented all the Essential Eight strategies but has also tailored them to the specific risk profile and business context of the organisation.
- **Proactive Stance:** The organisation takes a proactive approach to security, continuously reviewing and improving measures based on the changing threat landscape and business needs.
- **Advanced Adversary Protection:** At this level, the organisation is well-equipped to defend against targeted cyber-attacks by sophisticated threat actors.

Scoring for Each Strategy

The maturity model applies these levels to each of the eight strategies:

1. **Application control**
2. **Patch applications**
3. **Configure Microsoft Office macro settings**
4. **User application hardening**
5. **Restrict administrative privileges**
6. **Patch operating systems**
7. **Multi-factor authentication**
8. **Daily backups**

An organisation's overall maturity level is determined by the lowest maturity level scored across all eight strategies. For example, if an organisation scores at Maturity Level Two for seven strategies, but only Maturity Level One for one strategy, the overall maturity level would be One.

Progression Between Maturity Levels

- **Incremental Progress:** Organisations can progress through the maturity levels by incrementally strengthening their implementation of the Essential Eight.
- **Evidence-Based Scoring:** Scoring typically requires evidence of the effectiveness of implementations, such as policy documentation, technical controls, and audit results.
- **Continuous Improvement:** The maturity model encourages ongoing improvement and adaptation to emerging threats and business changes.

The Essential Eight Maturity Model scoring is integral to an organisation's cybersecurity strategy, as it provides a clear benchmark for their current posture and a roadmap for improvement.

A Look at the ASD Essential 8 Challenge

Application Control

Consensus Challenge:
Many small business leaders find the concept of application control important but struggle with the technical know-how of implementing and managing a whitelist system, especially as their business needs evolve and new software becomes necessary.

Elena, Partner at a Law Firm:
"I understand the importance of only using approved applications, but the how-to is a mystery. When we want to try new case management tools, it's a challenge. Not just understanding what whitelisting is, but also how to implement it as our needs evolve."

Patch Applications

Consensus Challenge:
Keeping applications up-to-date is recognized as crucial, but there's a significant challenge in managing these updates across a distributed team, particularly for businesses without dedicated IT support.

Michael, Managing Director of an Accounting Firm:
"Ensuring that our software is up-to-date is critical, especially with our team always on the move. The challenge isn't just technical; it's logistical. We all use the same financial software, but managing updates across multiple remote users is a task I'm not equipped for."

Configure Microsoft Office Macro Settings

Consensus Challenge:
Disabling macros in Microsoft Office applications is a recommended security measure that many find confusing or are unaware of how to implement correctly, leading to potential vulnerabilities.

Sarah, CEO of a Financial Planning Service:
"We know disabling macros is a security step, but no one on our team, including me, knows how to approach this. It's not just about the will to secure our systems; it's about the lack of clear, understandable guidance on how to do so."

User Application Hardening

Consensus Challenge:
The concept of hardening applications by disabling unnecessary features is often seen as complex and resource-intensive, particularly for small businesses without in-house technical expertise.

Liam, CEO of a Craft Brewery:
"The term 'application hardening' seems like it's from another world. With tight budgets, the prospect of hiring IT support is daunting. The real issue is making these concepts accessible and actionable for small businesses like mine."

Restrict Administrative Privileges

Consensus Challenge:
Limiting administrative access is a key security practice, yet many small businesses struggle with its practical implementation due to the collaborative nature of their work environments.

Carlos, Managing Partner of a Plumbing Business:
"We understand the need to limit access, but practically, it's difficult. Everyone pitches in on everything. The real dilemma is figuring out how to implement access controls without disrupting our workflow, considering we all need broad access to function effectively."

Multi-factor Authentication (MFA)

Consensus Challenge:
While MFA is widely acknowledged as a crucial security layer, small businesses face challenges in implementing it, especially when using shared accounts or addressing staff concerns about using personal devices.

Jordan, Managing Director of an Accounting Firm on Shared Access:
"Client demands sometimes necessitate shared logins. Implementing MFA in such scenarios seems impractical. The real issue here is finding a security model that accommodates shared use without compromising security."

Alex, Partner at a Financial Planning Firm on MFA and Personal Devices:
"My team is wary of using personal devices for MFA, and outfitting everyone with company phones is not feasible. The challenge extends beyond security measures; it's about finding cost-effective solutions that respect personal boundaries and practicality."

Patch Operating Systems

Consensus Challenge:
Regularly updating operating systems is essential for security, yet small business leaders often find it challenging to ensure consistent updates across all devices, particularly for teams that are frequently mobile.

Elena, Partner at a Law Firm:
"Keeping our systems up-to-date is undeniably important, but doing so consistently, especially with a mobile team, is challenging. The real issue is finding a manageable approach to ensure all devices are secure, not just understanding the importance of updates."

This approach highlights the real challenges small business leaders face in understanding and implementing the ASD Essential 8 cybersecurity strategies, emphasizing the gap between theoretical best practices and the practical realities of running a small business.


SECURITY IN DEPTH