
SECURITY IN DEPTH
Cyber Awareness
The ever-evolving landscape of cybersecurity threats

Presenter

Michael Connory
Security in Depth - CEO

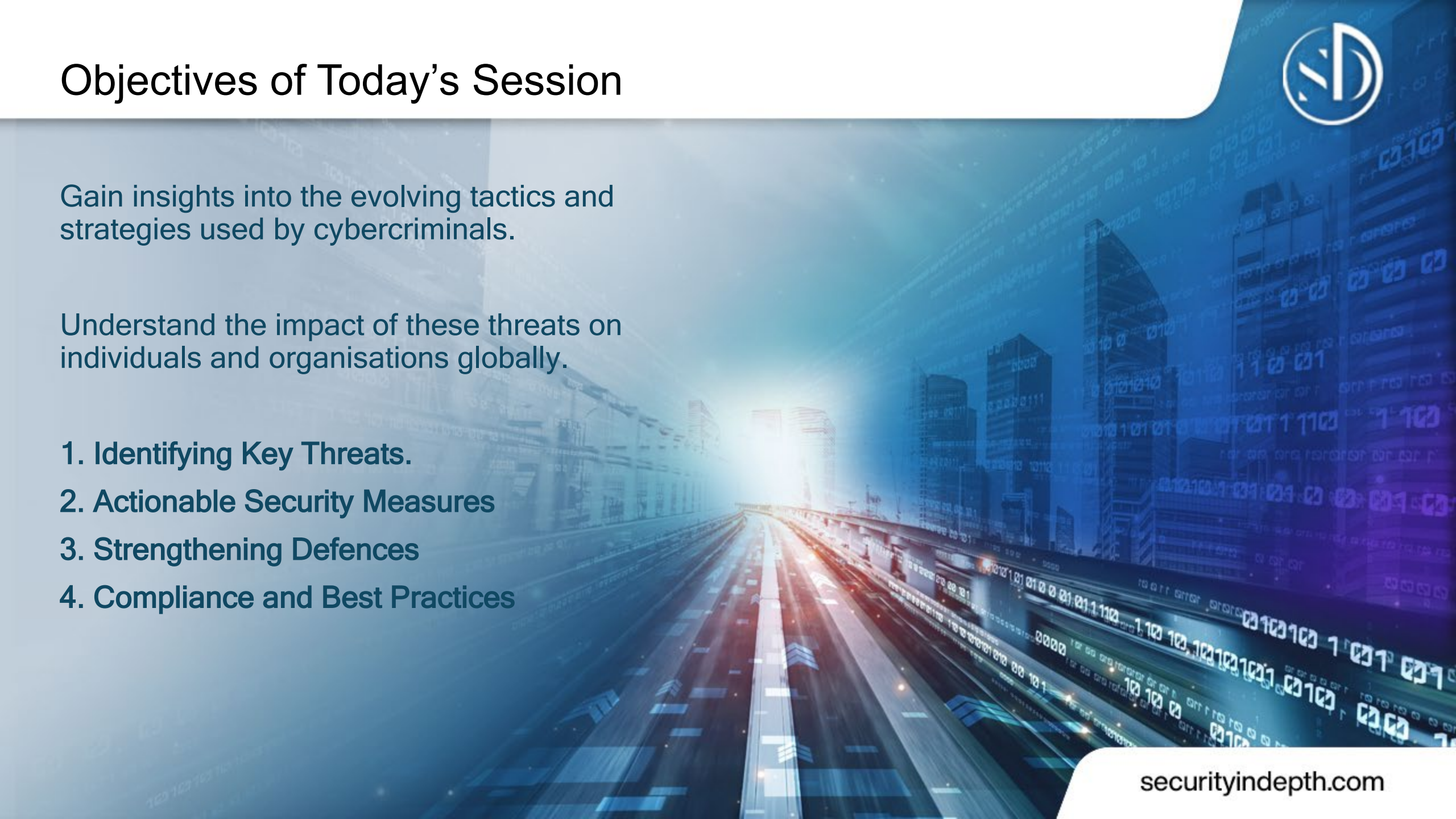
securityindepth.com

Objectives of Today's Session

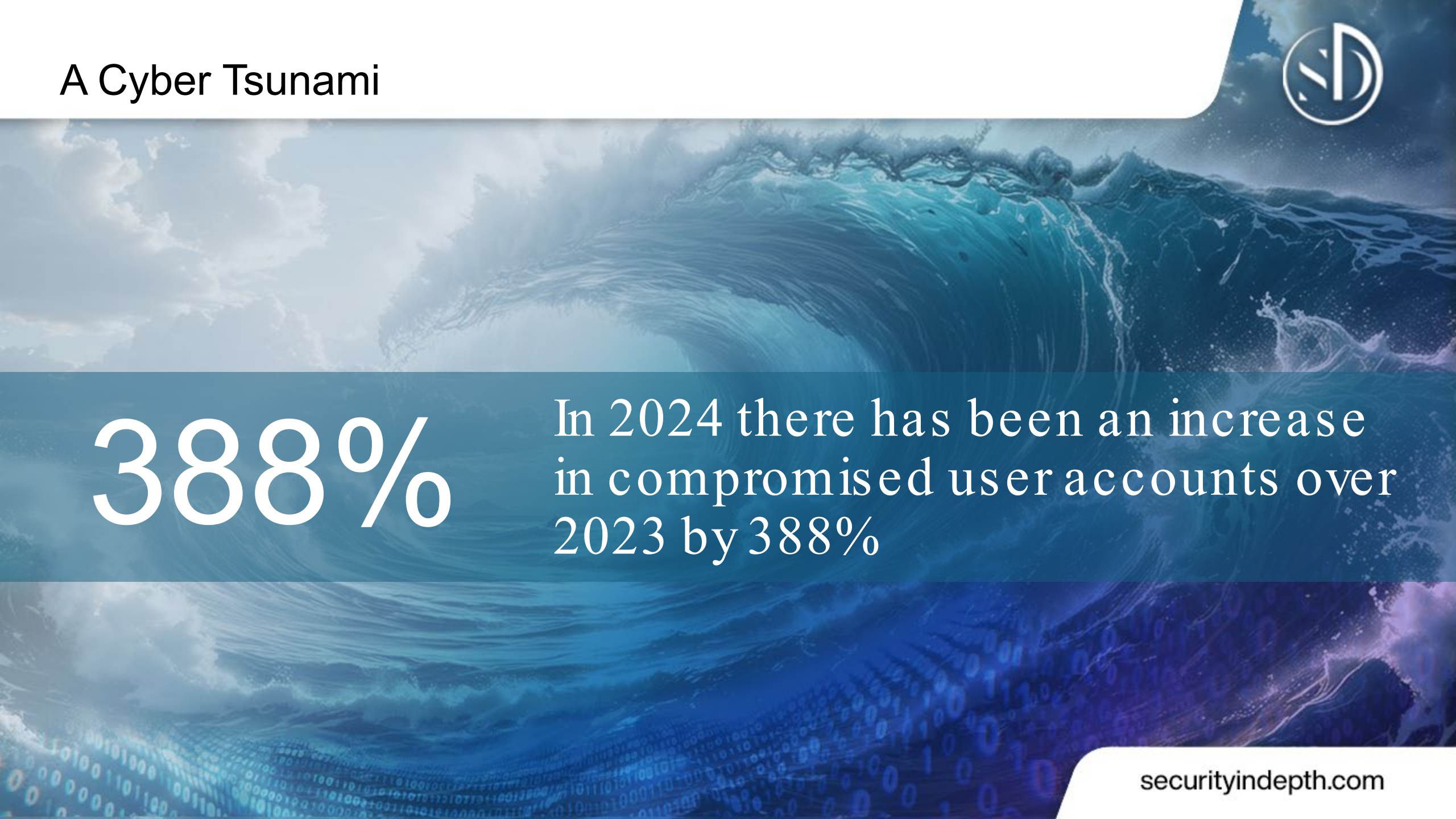
Gain insights into the evolving tactics and strategies used by cybercriminals.

Understand the impact of these threats on individuals and organisations globally.

1. Identifying Key Threats.
2. Actionable Security Measures
3. Strengthening Defences
4. Compliance and Best Practices



A Cyber Tsunami



388%

In 2024 there has been an increase in compromised user accounts over 2023 by 388%

It Never Stops

Since 2004 an average of 13 accounts in Australia are compromised every minute

6,832,800

Over the last 12 months
6,832,800 Australian accounts
have been compromised

Money Lost Forever

$2,700,000,000 Stolen over the last 12 months

securityindepth.com

The Current Cyber Threat Landscape

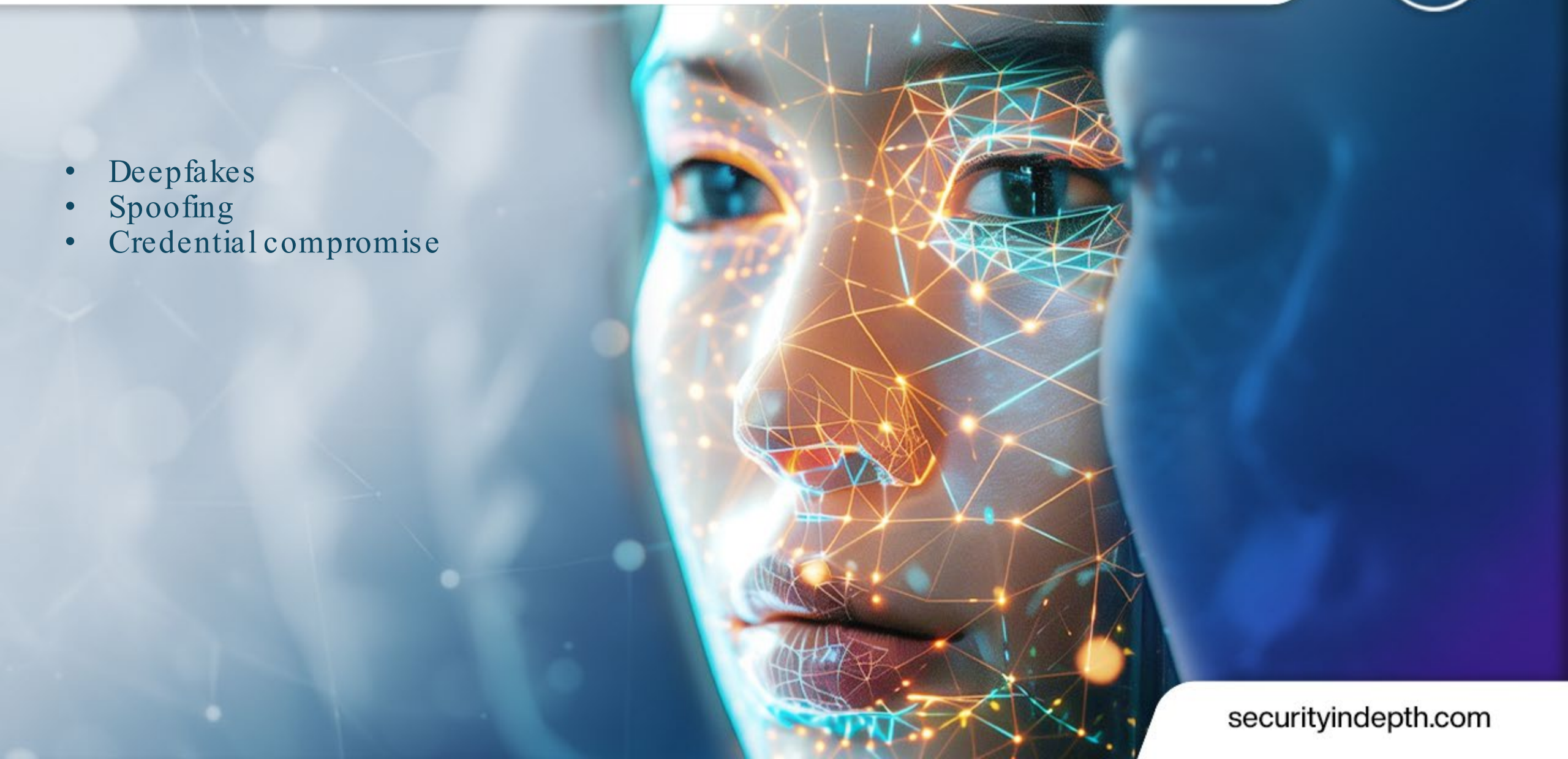
Common cyber threats:

- Ransomware attacks.
- Social Engineering.
- Phishing scams.

552,000 | Cyber Incidents Reported in 2023

The New Threats

- Deepfakes
- Spoofing
- Credential compromise



The Cyber Rainbow

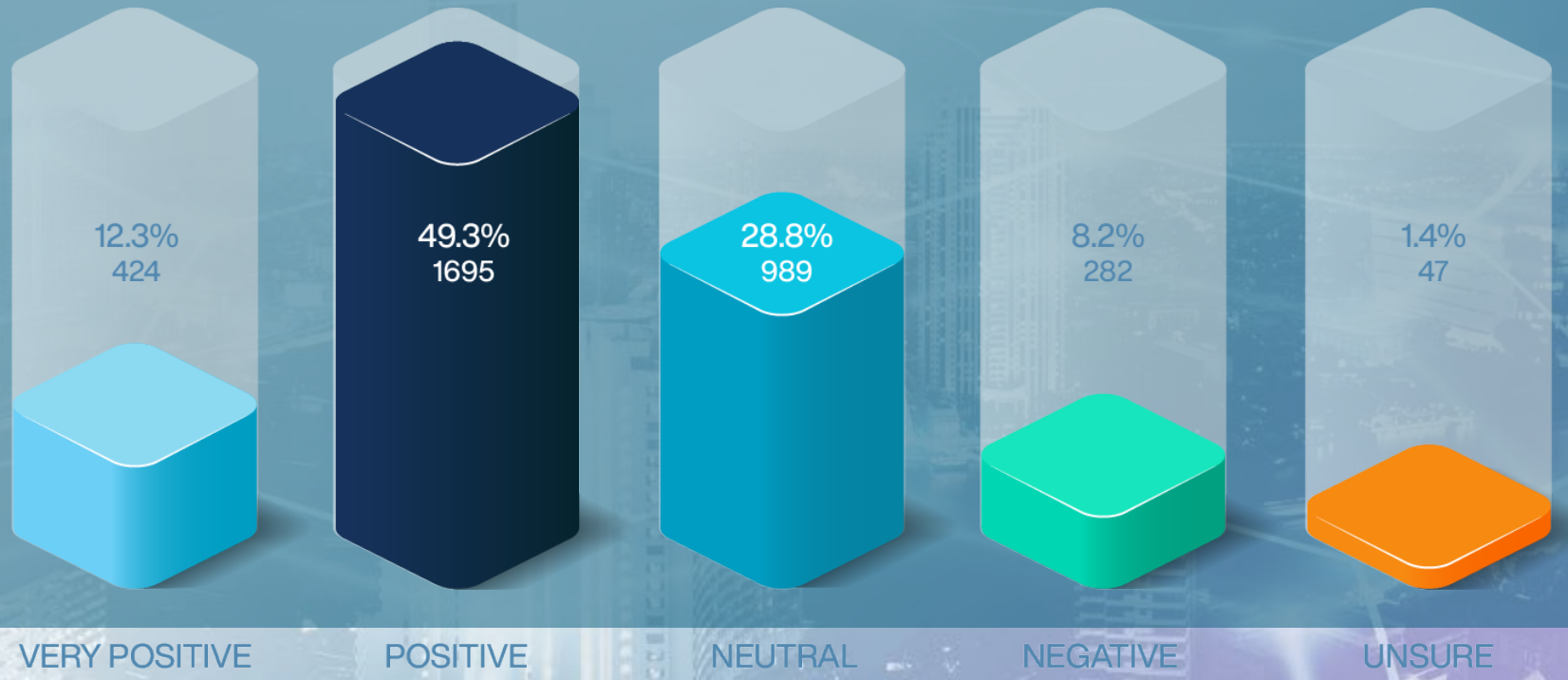
There are a huge number of small actions that can help protect you


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

QUESTION:

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

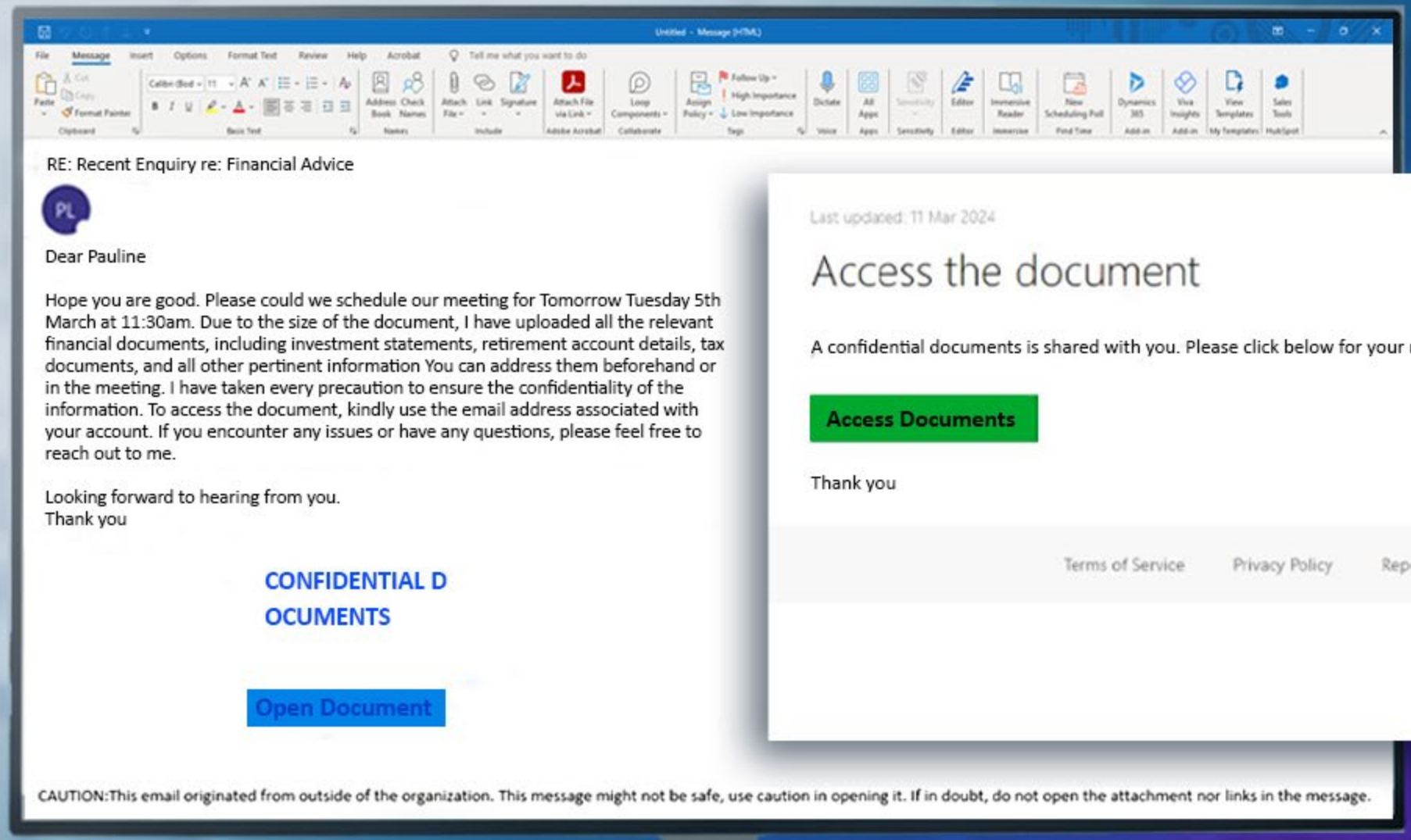
The data reveals that respondents have varied levels of confidence in their organisation's cyber resilience.



Phishing Attacks

AI is now part of the strategies

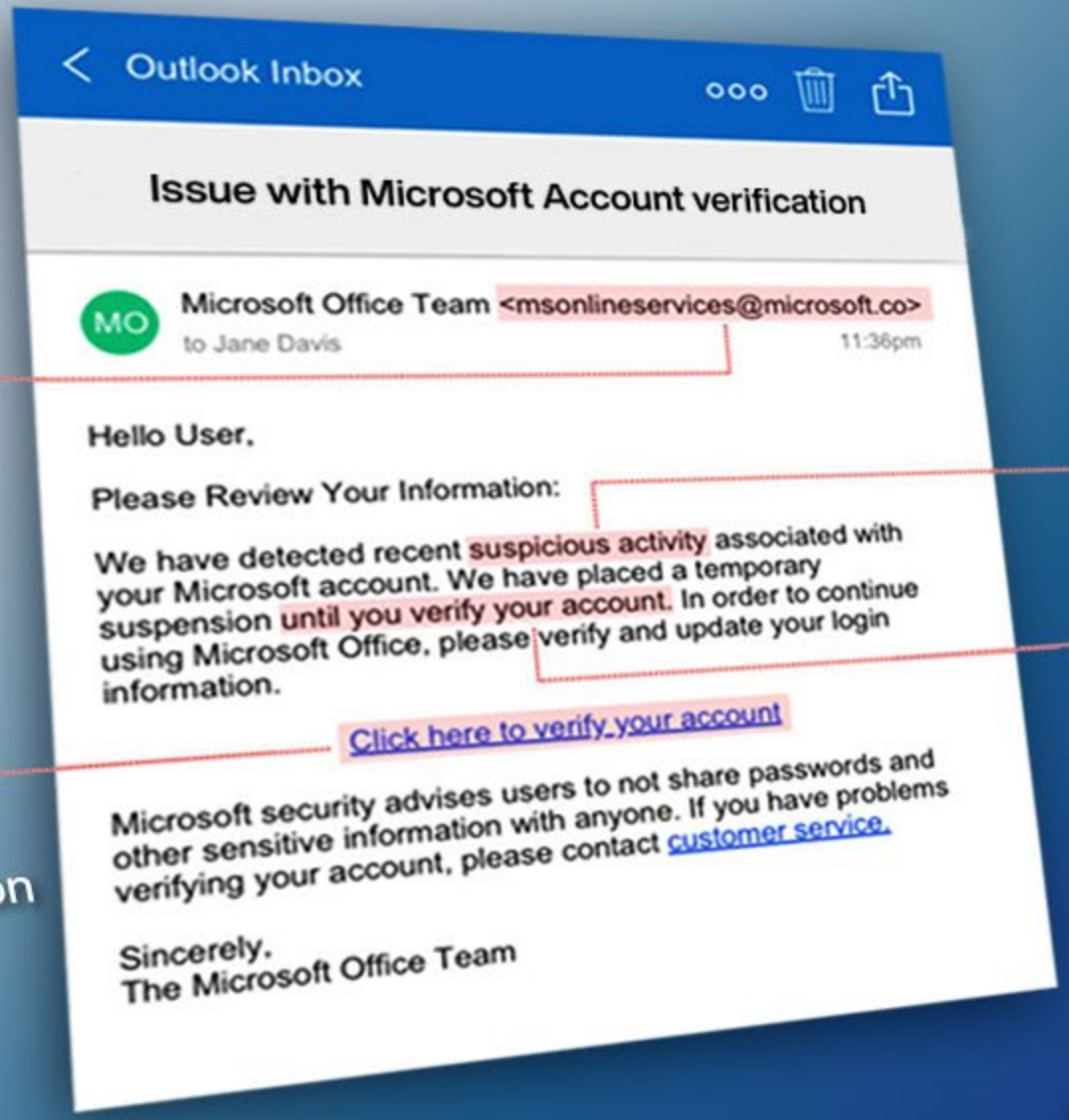
Phishing Attacks Samples



Email Spoofing

securityindepth.com

Email Spoofing Samples



Spoofed Email address

Attention Grabber

Sense of Urgency to cause panic

Attacker hides the malicious link with verification button

Your Clients are a challenge

- Not using MFA
- No Password management
- Reusing passwords
- Believe you are responsible

Client Files are the new Digital Currency

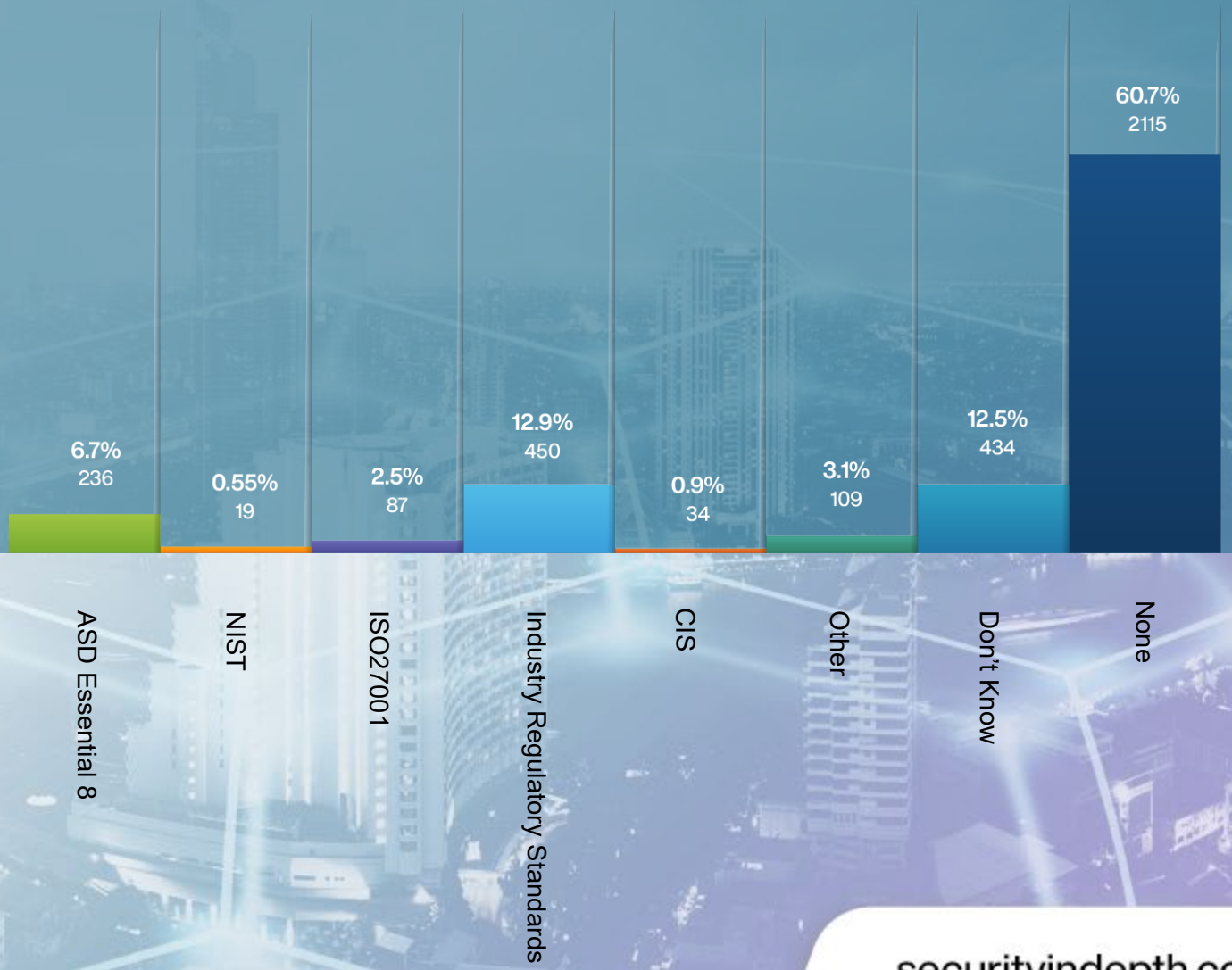
Let me tell you a Story

- Aged Care Home
- Docusign
- Superannuation

GOVERNANCE

QUESTION:

Does your organisation adhere to an IT Security framework?

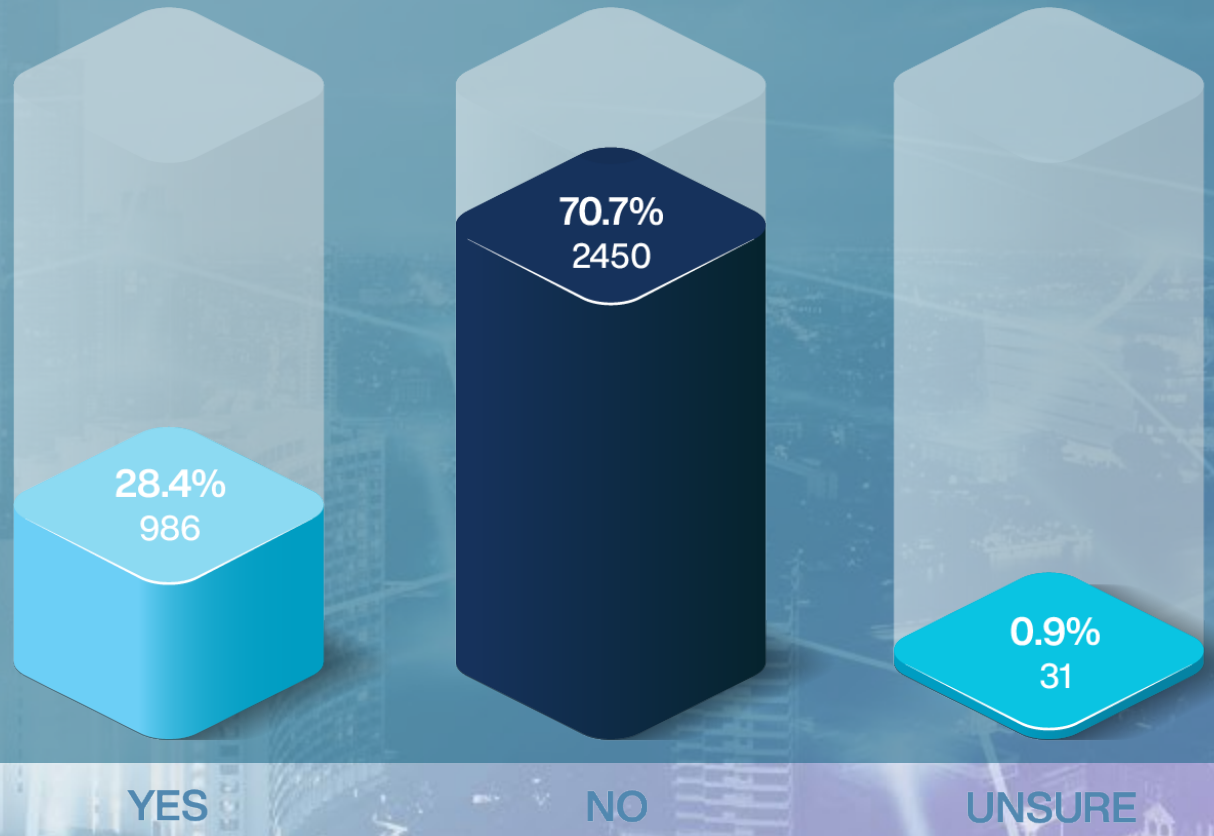


The diverse adoption of IT security frameworks among surveyed Australian organisations highlights the need for greater awareness, education, and resources to support the implementation of comprehensive cybersecurity practices.

QUESTION:

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

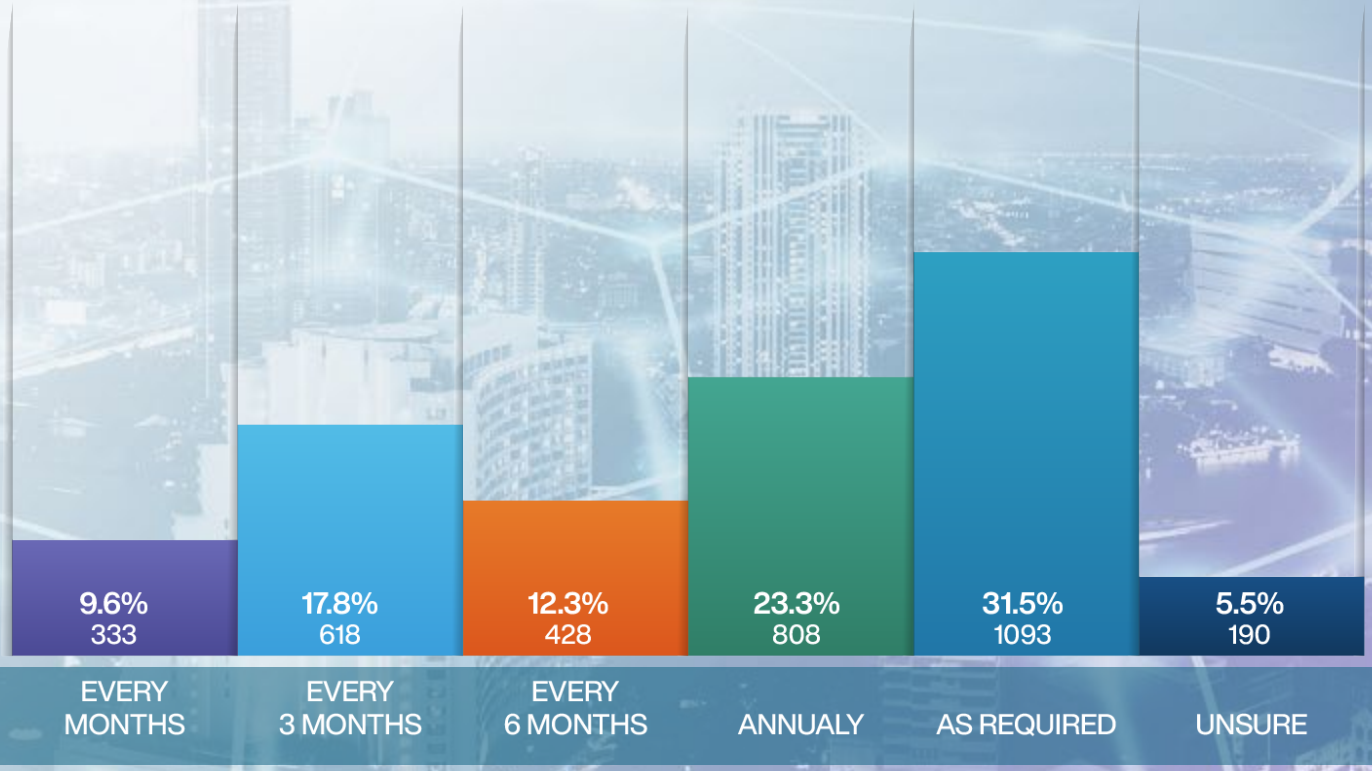
The data presented reveals that only 28.44% of organisations have engaged an independent party to audit their computer systems and processes.



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.

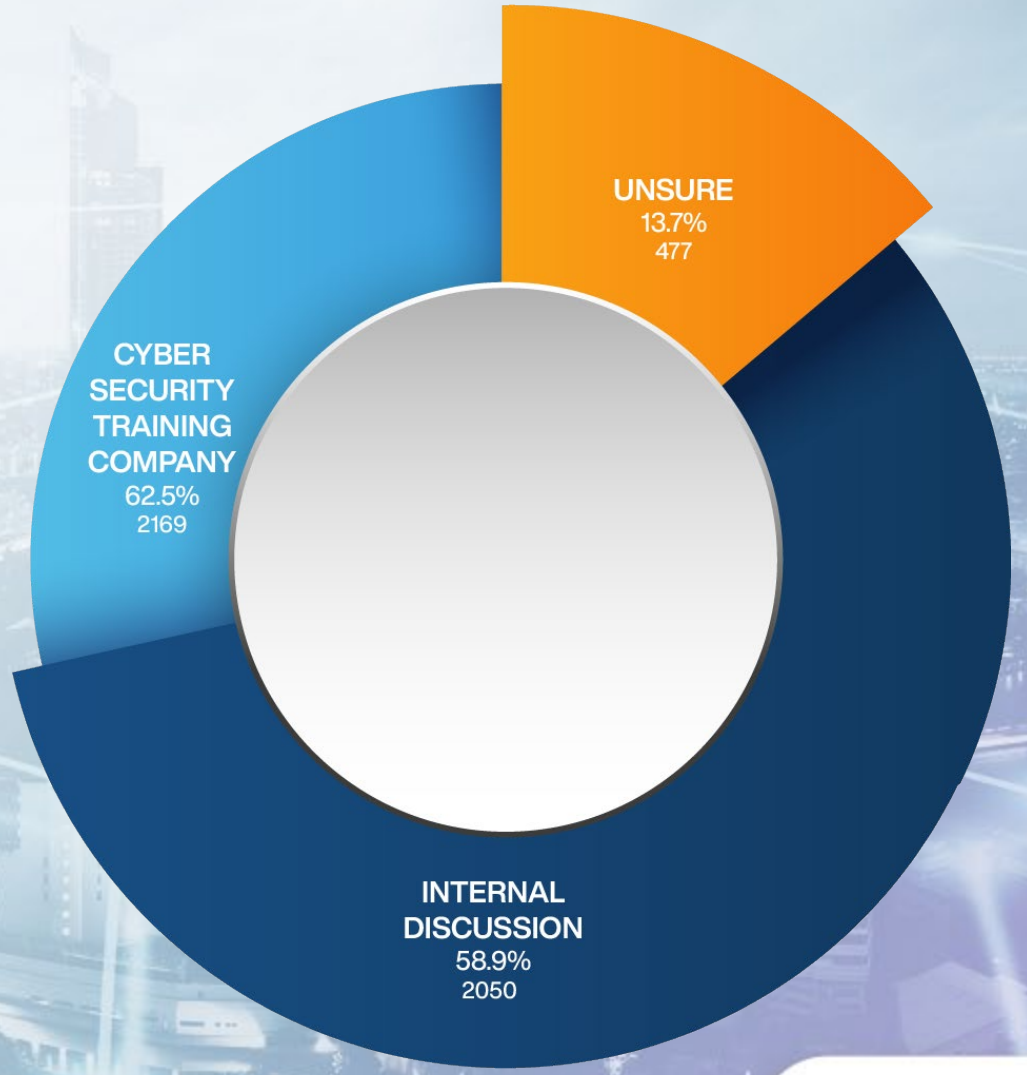


QUESTION:

How do you conduct cyber security awareness training?

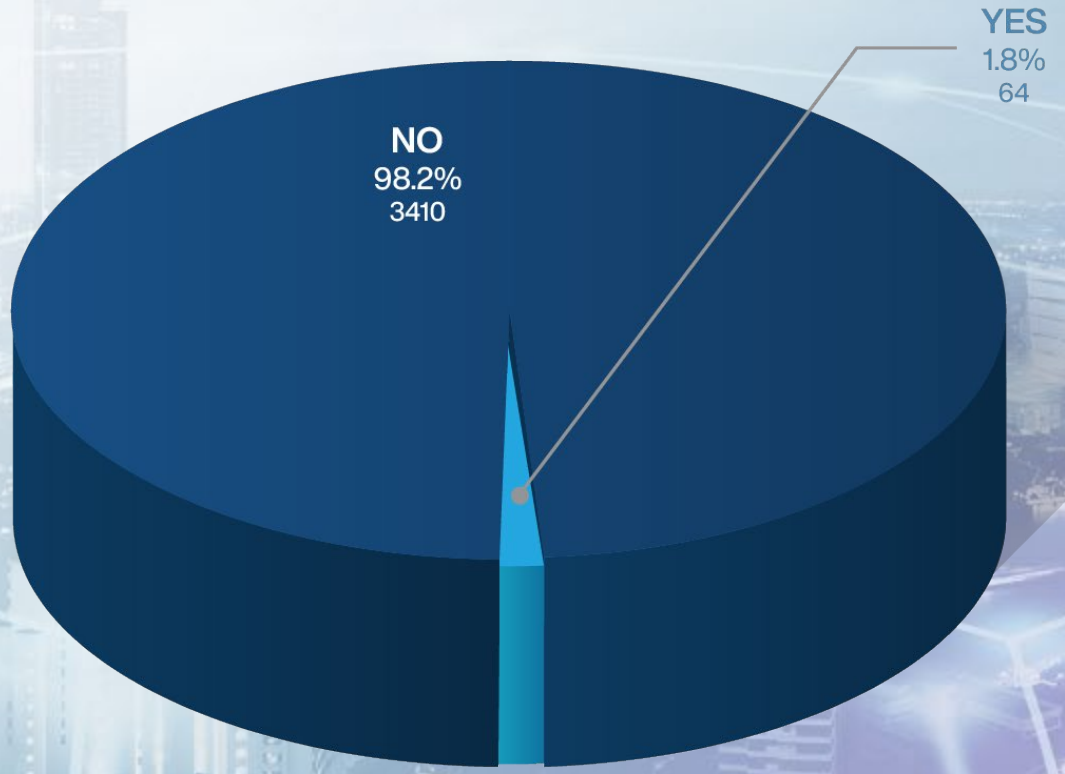
The survey sheds light on the methods through which organisations conduct cybersecurity awareness training.

A majority, 58.9%, 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.



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.

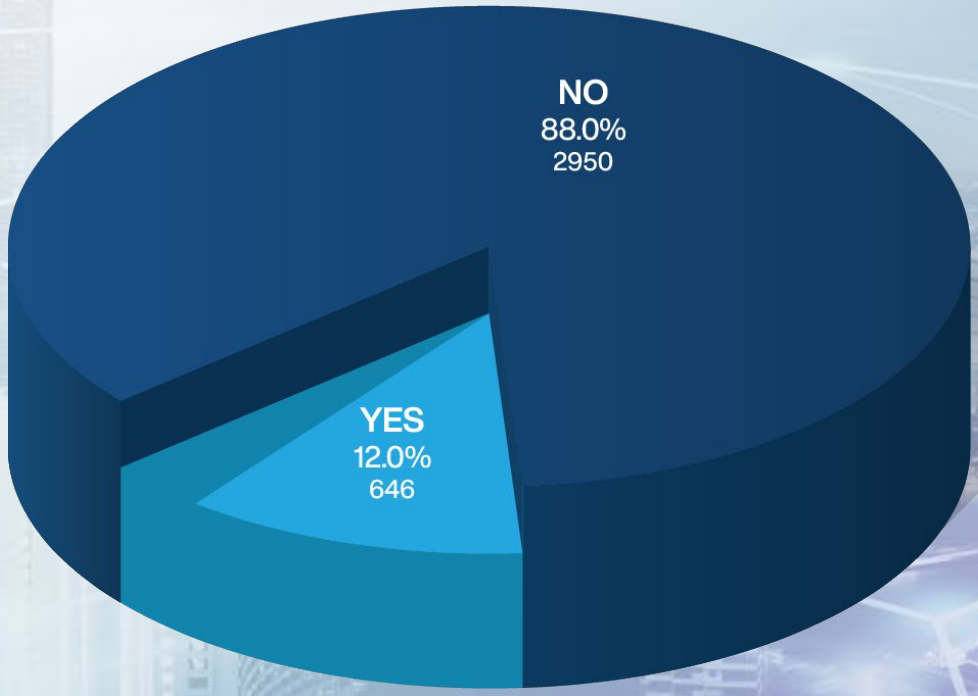
When considering that only 22.10% of respondents have a written cyber incident response plan, the additional data point that a mere 1.84% have fully tested their plans with an external organisation is even more alarming.

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.

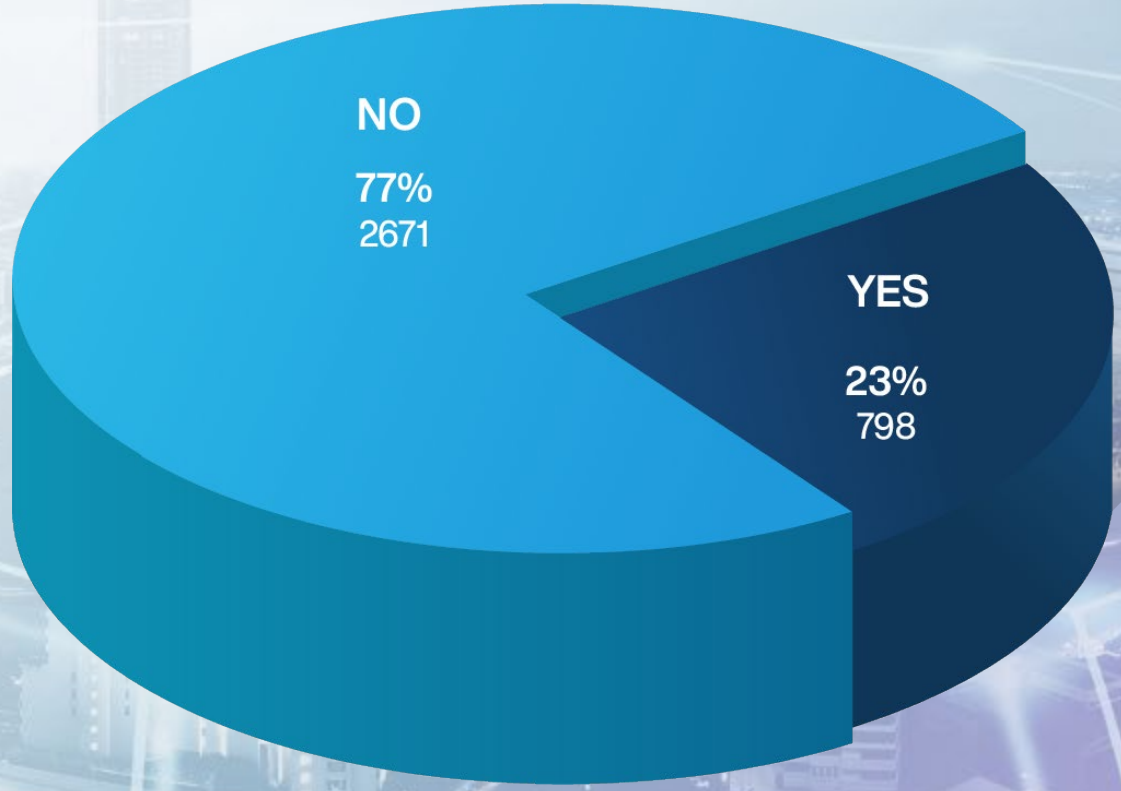


TECHNICAL

QUESTION:

Does your organisation monitor for reused passwords?

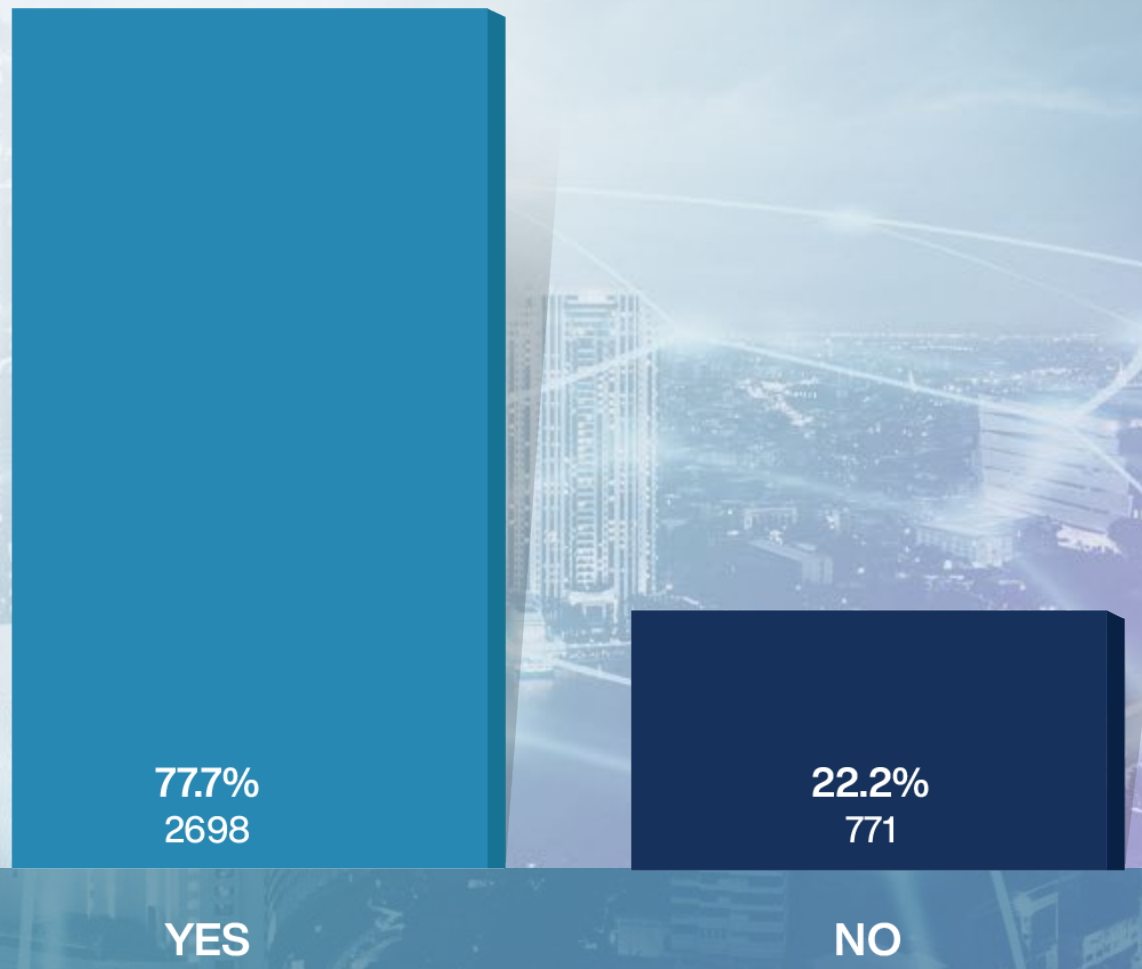
The survey reveals that only 23% of organisations actively monitor for reused passwords. This is a critical cybersecurity practice, and the fact that 77% of respondents do not engage in this monitoring is concerning.



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.



QUESTION:

Do you reuse business and personal passwords?

The information from the 2024 State of Cyber Security Survey shows a strikingly high rate of password reuse among respondents, with 92% indicating they reuse business and personal passwords.

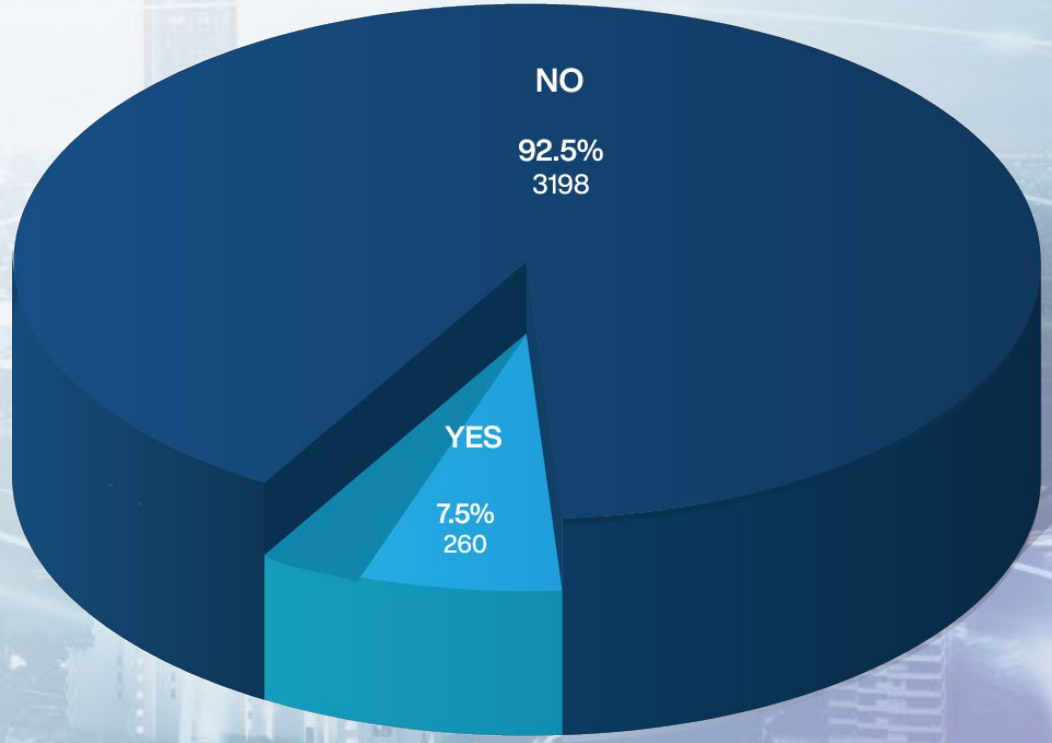
This practice exposes both personal and professional systems to a higher risk of security breaches, as compromised credentials in one area can lead to unauthorized access in another.

Technical

QUESTION:

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

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.

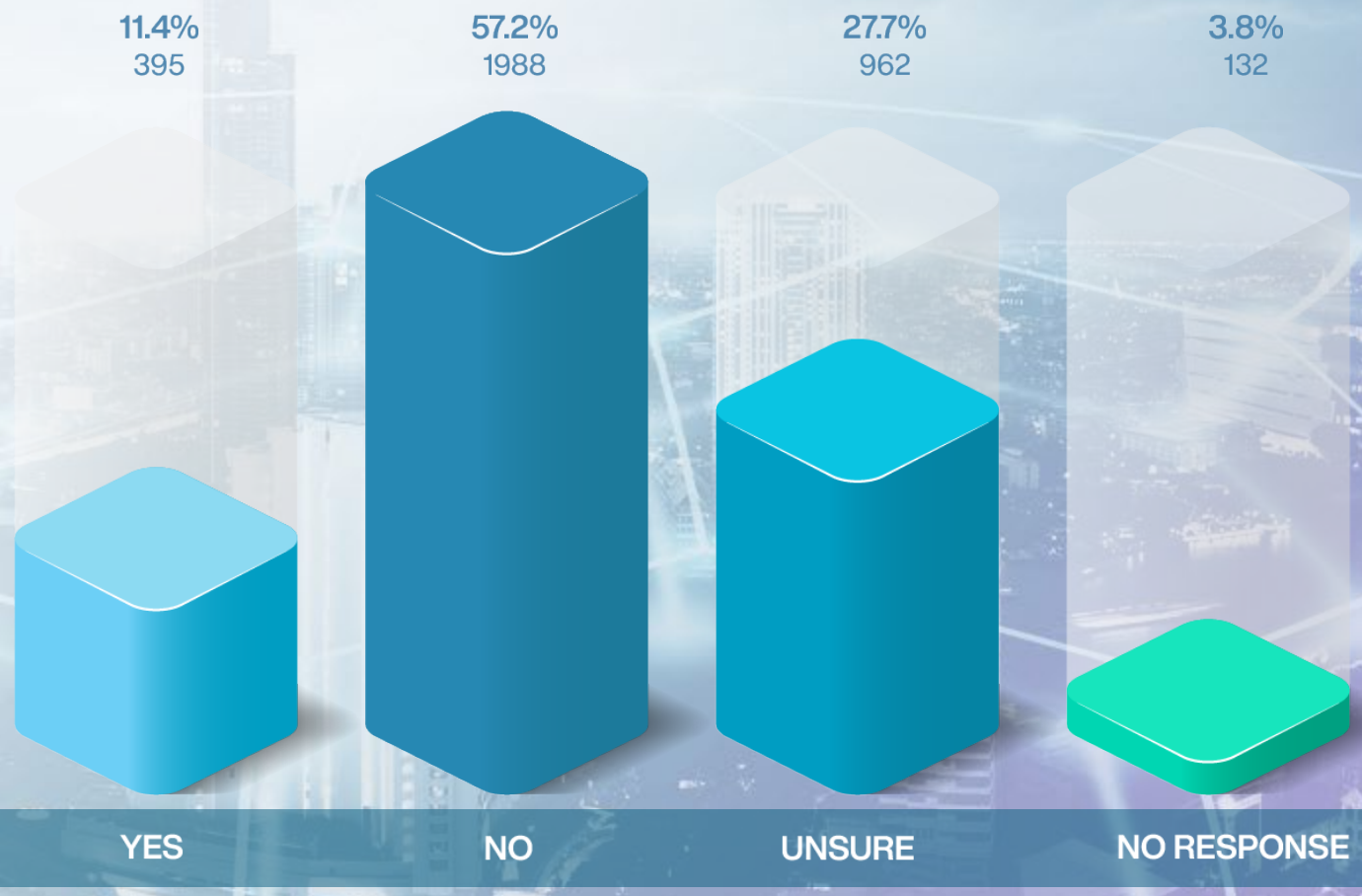


QUESTION:

Does your environment utilise MDM?

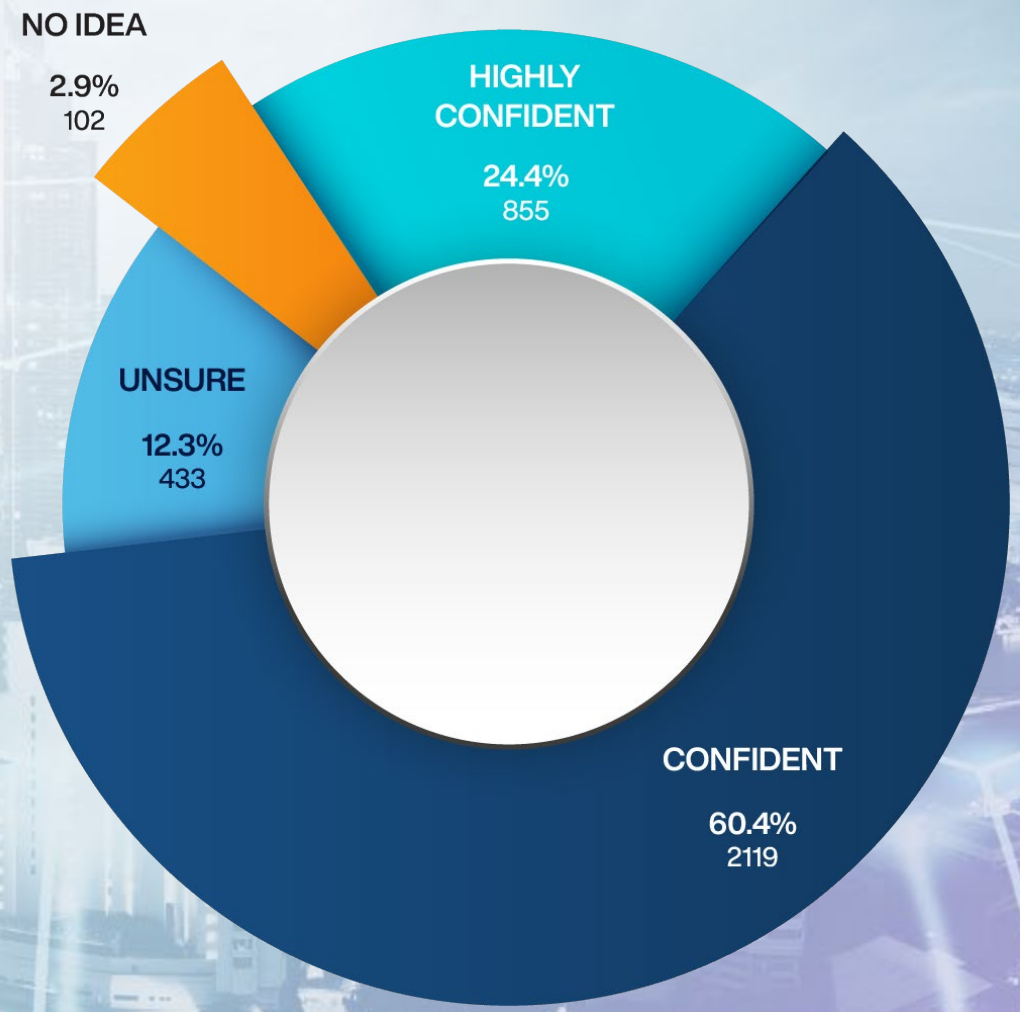
(Mobile Device Management)

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.



QUESTION:

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



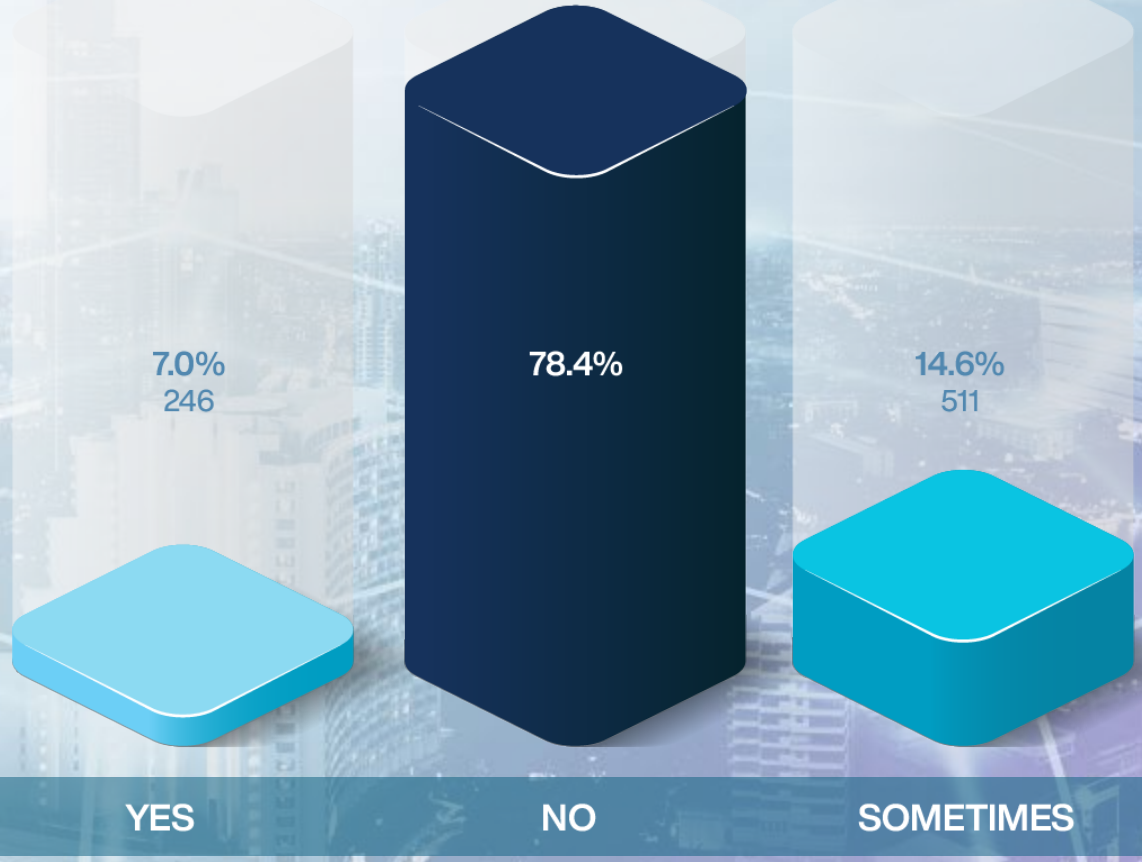
A substantial 84.76% of respondents exhibit confidence, with 24.37% asserting high confidence and 60.39% expressing general confidence. This data may reflect the positive impact of cybersecurity awareness campaigns and educational programs that aim to equip the public with the knowledge and skills necessary to recognize and avoid cyber threats.

QUESTION:

Do you report Phishing emails when recognised?

The data presented here paints a concerning picture about the reporting behaviors related to phishing emails.

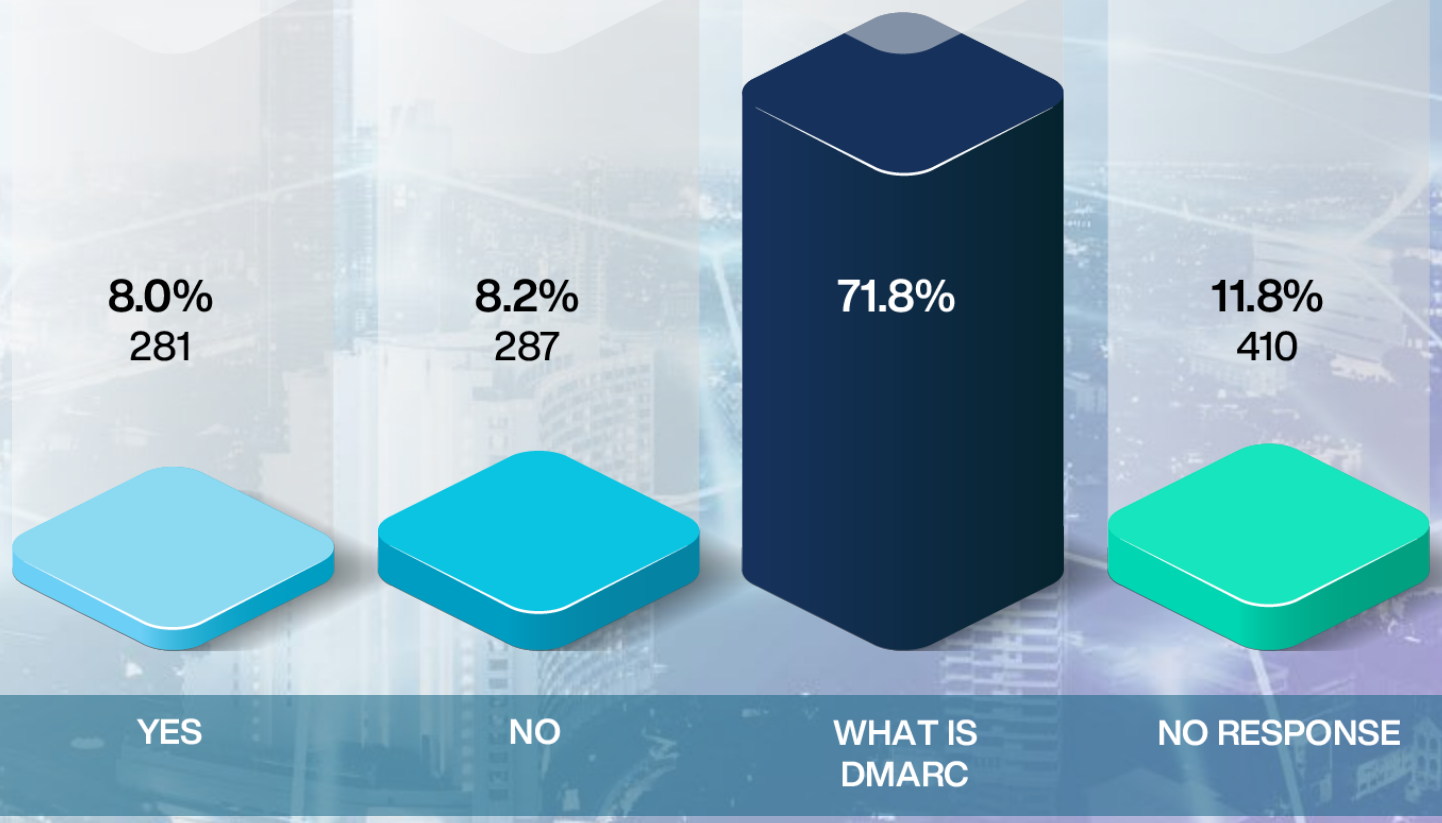
Despite a previous indication that a majority of respondents are confident in identifying phishing emails, a substantial 78.43% admit they do not report phishing emails when recognized. This disparity raises significant questions about the effectiveness of cybersecurity awareness and the actual practices of email users.



QUESTION:

Does your Business utilise DMARC to prevent domain spoofing?

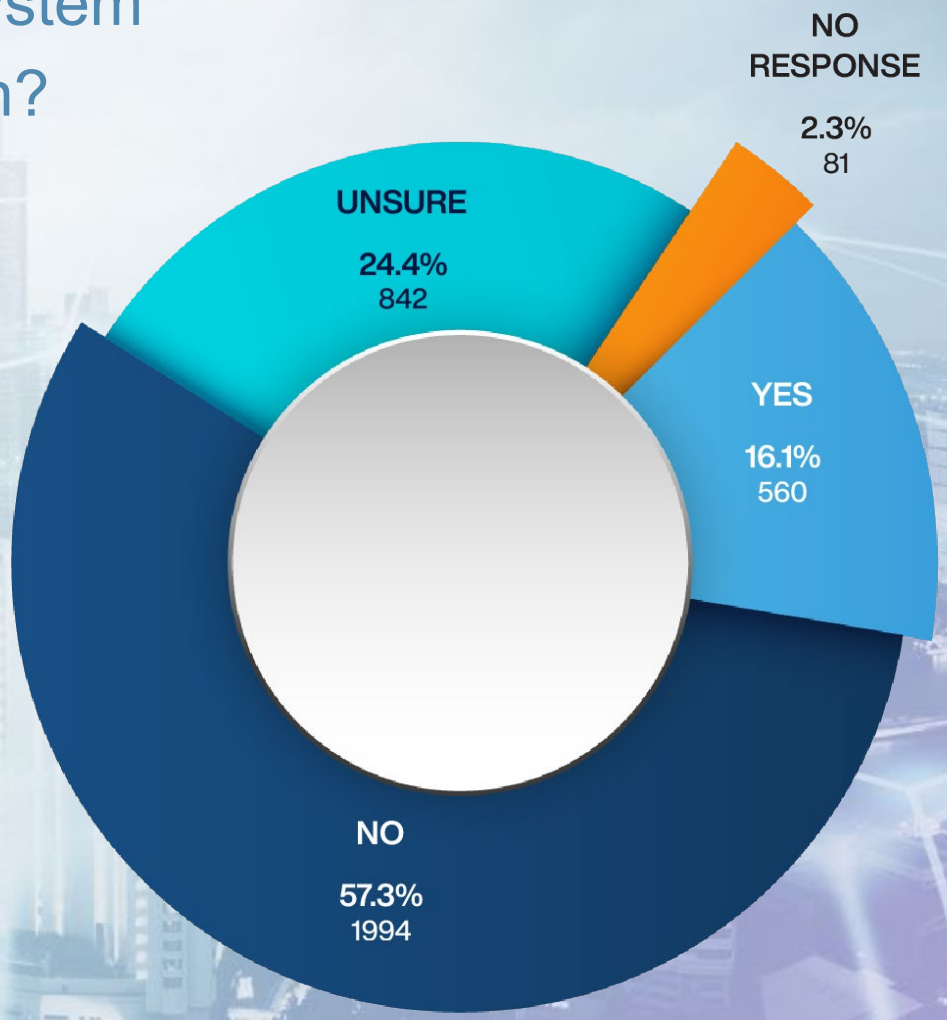
The data concerning the use of DMARC (Domain-based Message Authentication, Reporting, and Conformance) for preventing domain spoofing among businesses reveals several notable points.



QUESTION:

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

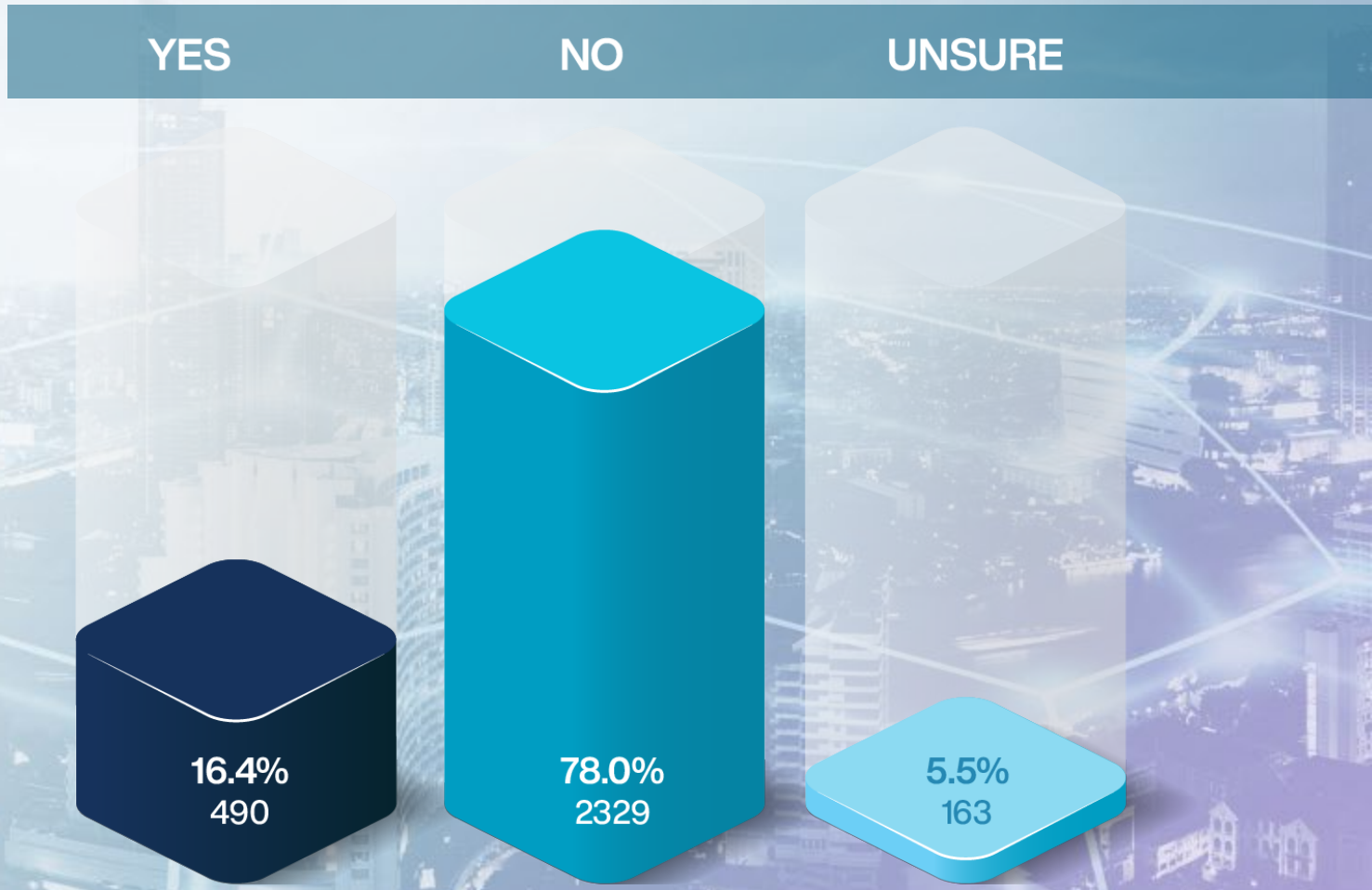
In conclusion, the data points to a notable lack of active system monitoring within a majority of the organisations represented. Given the critical role of monitoring in detecting and responding to cybersecurity incidents, the findings highlight a significant area of potential improvement for organisational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



Technical

QUESTION:

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

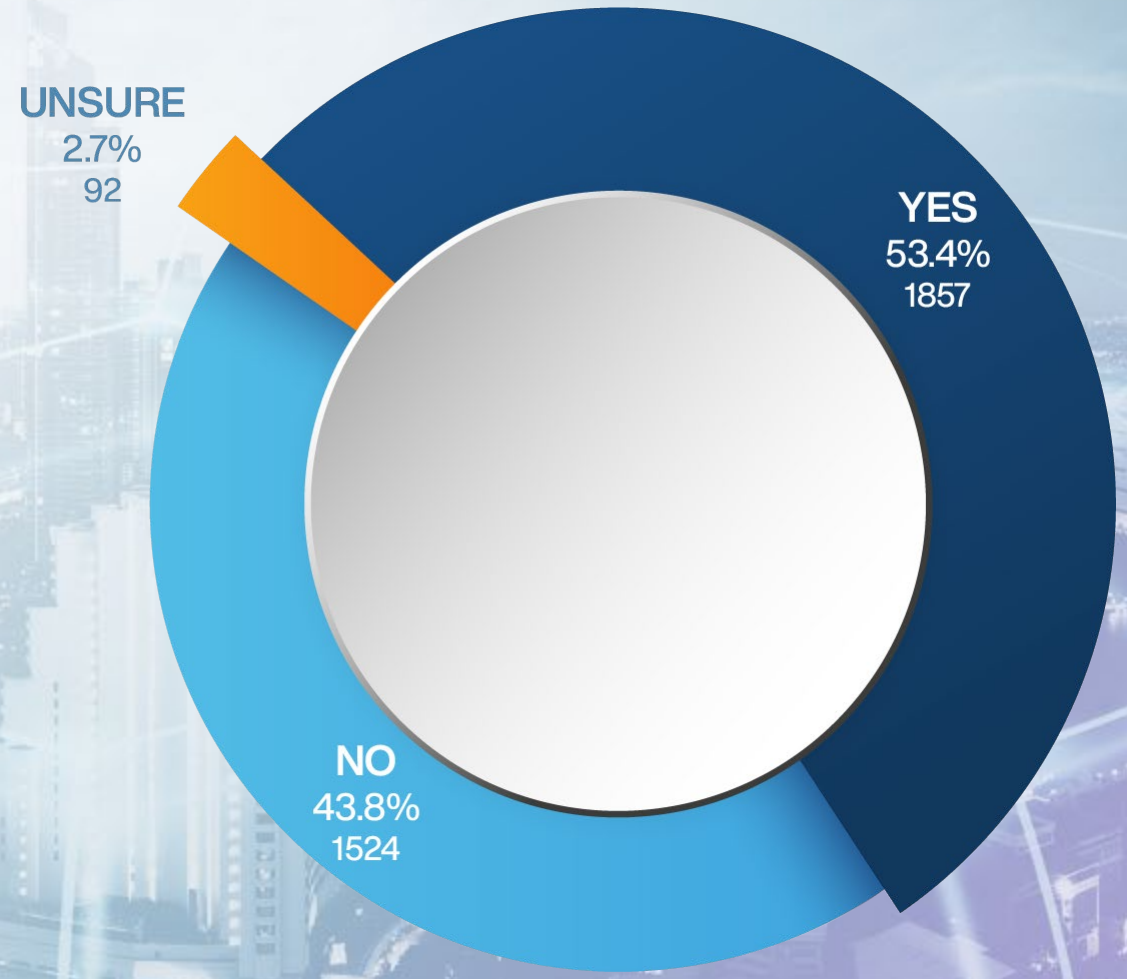


Considering the previous data on system monitoring and DMARC usage, this paints a troubling picture of the overall cybersecurity posture across various organisations.

THIRD PARTIES

QUESTION:

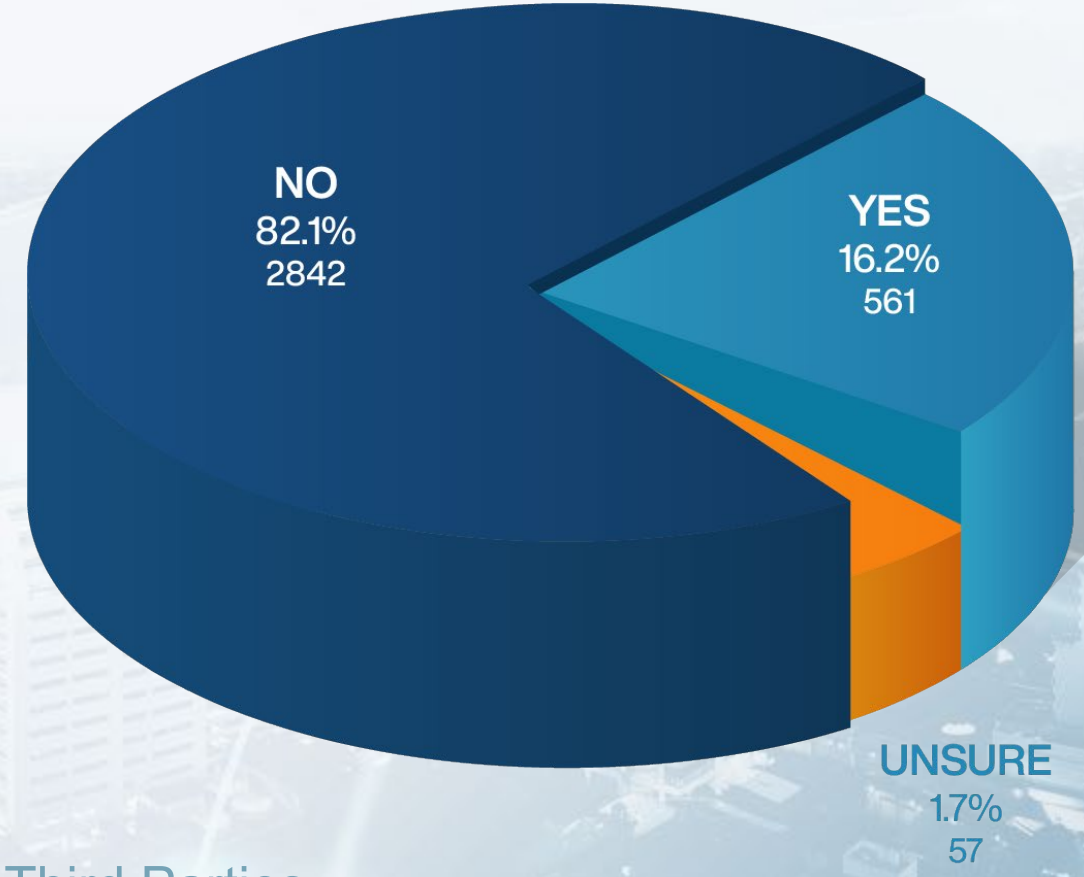
Do you outsource your IT to a Managed Service Provider?



The survey indicates that a majority of the respondents, 53.4%, 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, 43.8% retain their IT operations in-house, while a small portion, 2.7%, are unsure about their IT management structure.

QUESTION:

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



The data presents a concerning picture: only 16.2% of respondents have seen or reviewed the cybersecurity capabilities of their IT provider.

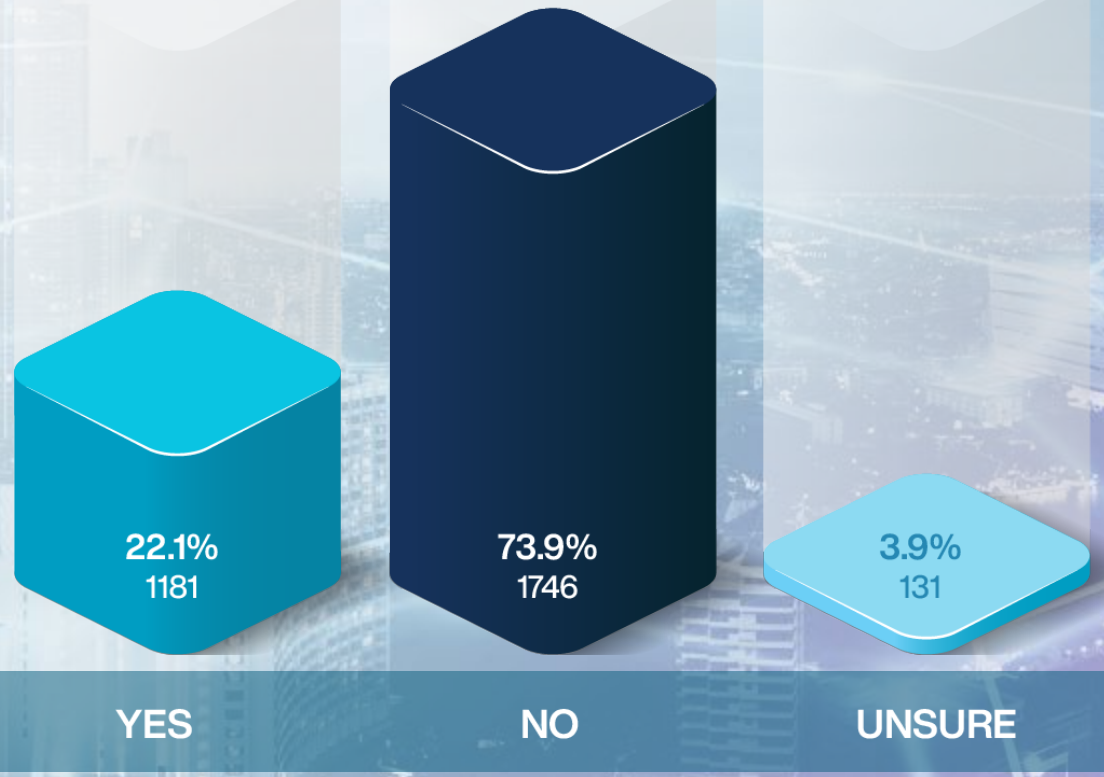
This leaves a vast majority, 82.1%, who have not, with a small percentage, 1.6%, unsure about whether they have undertaken such a review.

INCIDENTS

QUESTION:

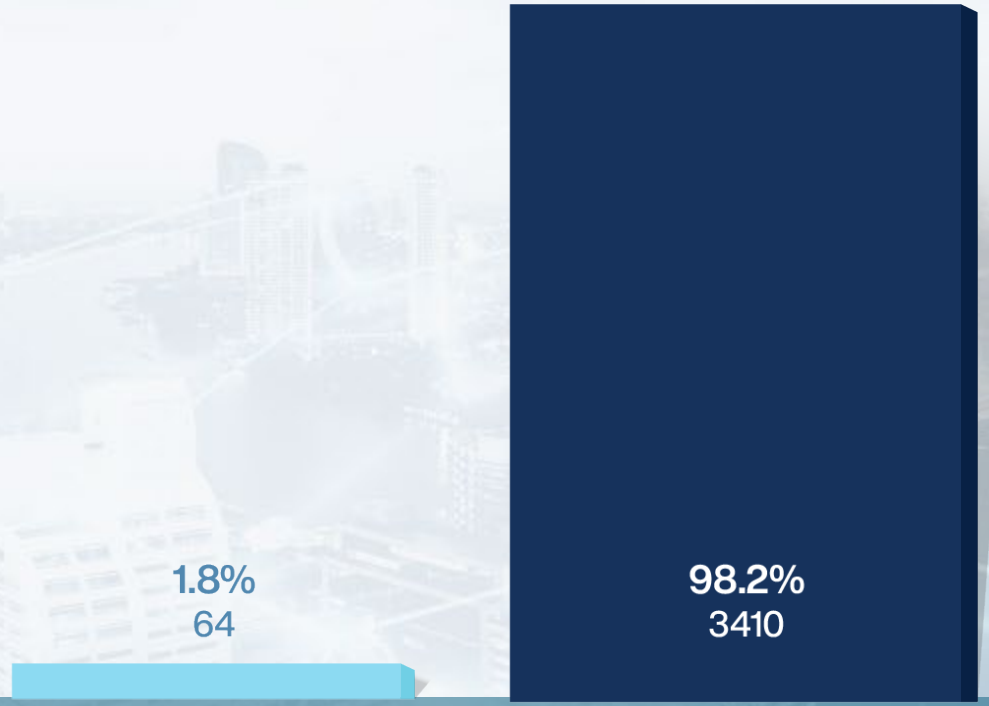
Do you currently have a written cyber incident response plan?

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.



QUESTION:

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



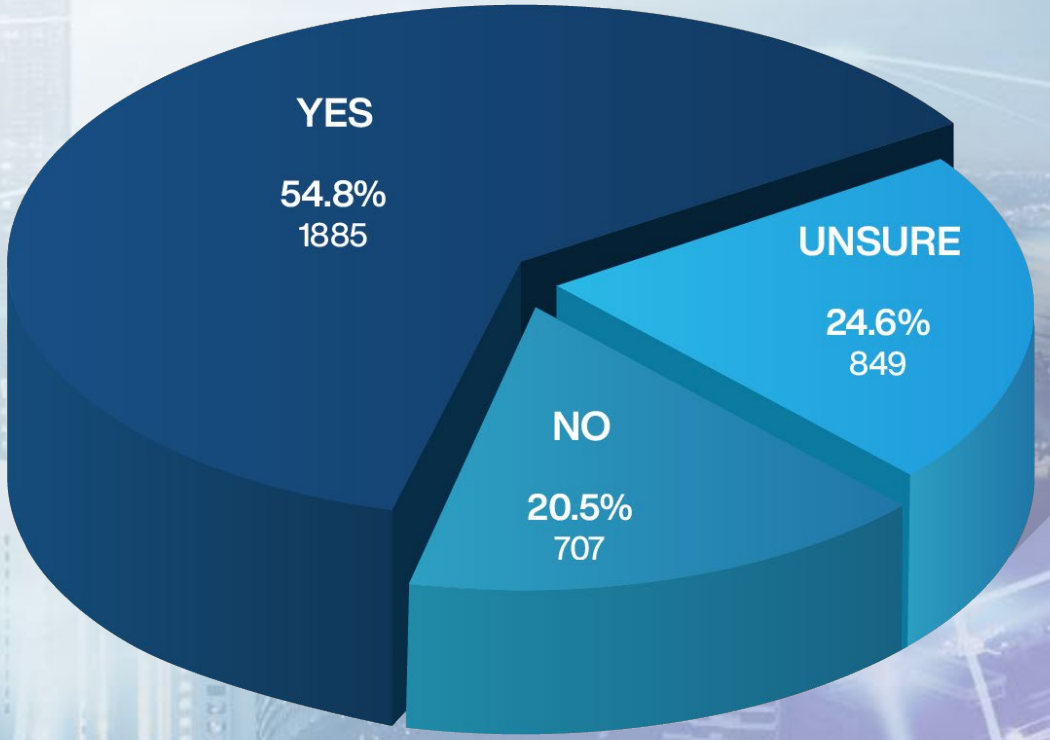
The survey responses here highlight a critical shortfall in cybersecurity readiness across surveyed industries. When considering that only 22.10% of respondents have a written cyber incident response plan, the additional data point that a mere 1.84% have fully tested their plans with an external organisation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

Incidents

QUESTION:

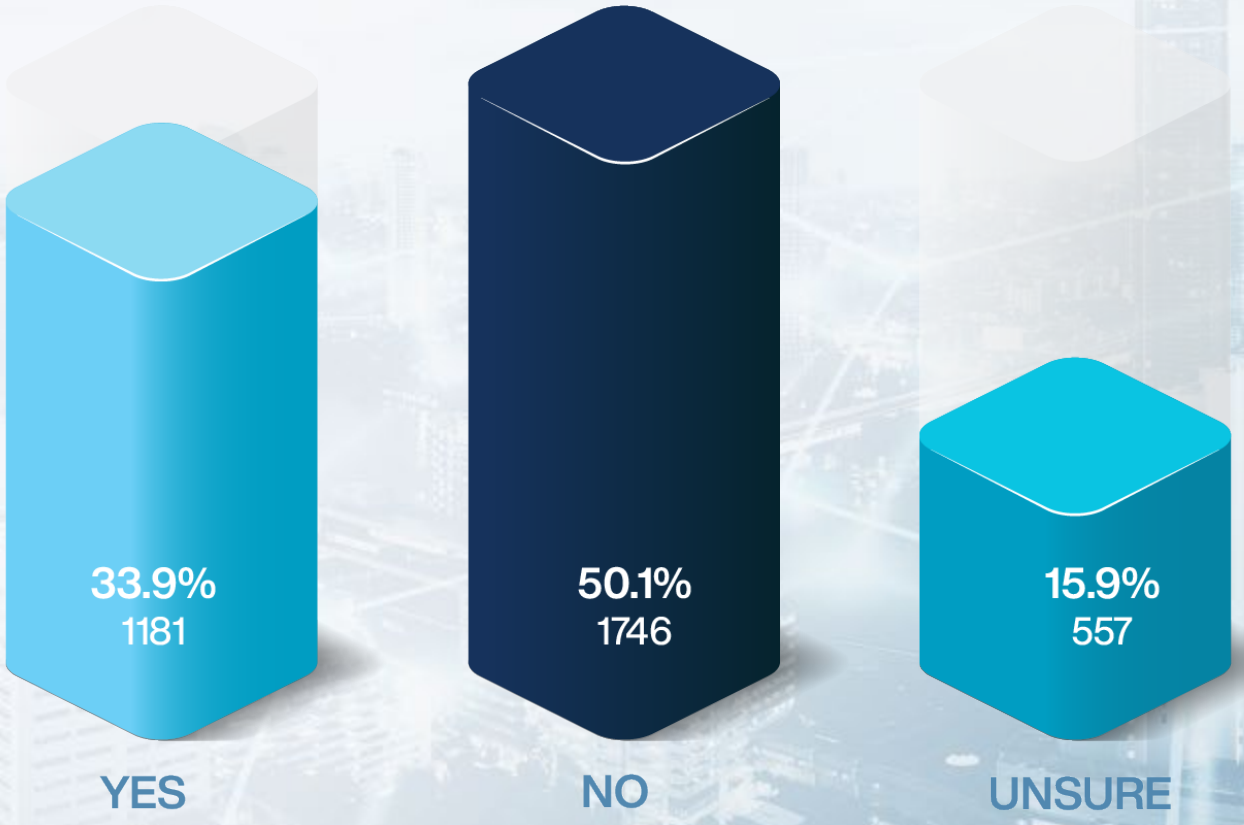
Does your organisation have the skills needed to respond to and recover from a cyberattack?

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.



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.

Laptop Left in Car

Company Broken Into

The Mercedes Story

What can be done?

- Teach your clients Cyber Safety
- Enforce MFA
- Utilise Client Portals for Sharing Informations
- DMARC
- Processes for Double Checking Everything

Questions?

Contact Us

SECURITY IN DEPTH

1300 041 042

support@securityindepth.com


THANK YOU
SECURITY IN DEPTH