ManageEngine

How cyber resilient are organisations in ANZ?

Cybersecurity and PII Report

Index

Introduction

The Cybersecurity and PII Report by ManageEngine investigates the extent to which modern organisations value, uphold and implement cyber readiness in all aspects. 306 IT decision-makers from different organisations in ANZ were surveyed, covering topics such as cyber resilience, personally identifiable information (PII) management, cyber practices under hybrid work models, the Essential Eight, malware, and ransomware. The report consolidates various insights from the respondents, that can aid key stakeholders in building futuristic businesses that are cyber secure from the core, and help accomplish a digital society that is always prepared.

Overview

In August 2023, 306 IT decision-makers (ITDMs) answered questions on a range of issues for ManageEngine. Research participants were selected from an online permission-based research panel. This sample size gives a confidence level of ± 5.6% at the 95% confidence level.

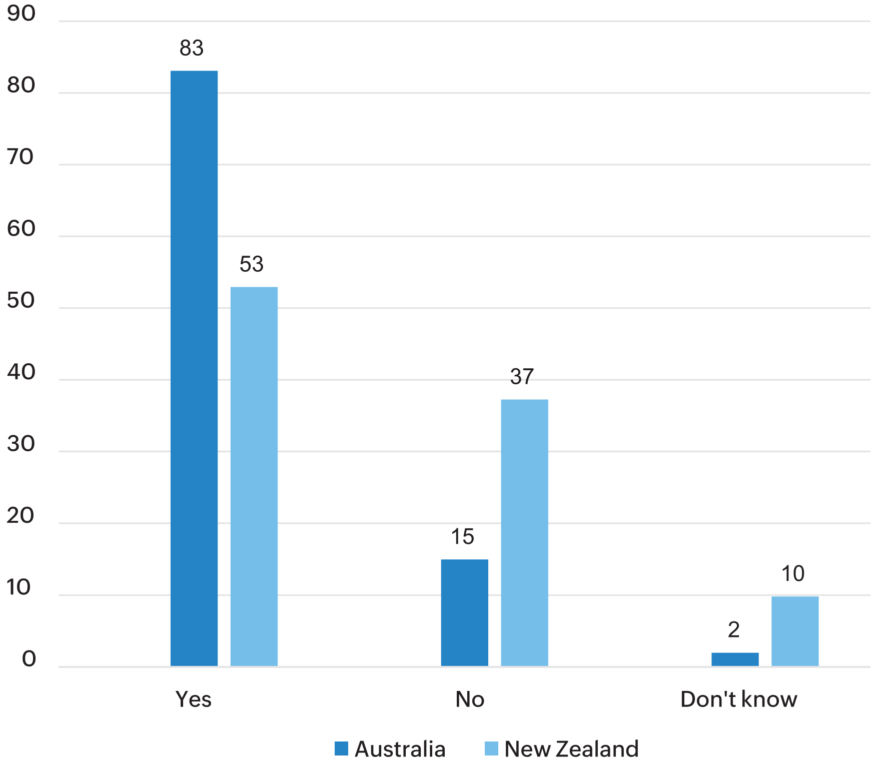
Who are ITDMs?

ITDMs provide inputs into IT decision-making for organisations and can be sole decision makers or designated teams that make IT recommendations. This includes people working in the IT department, senior management from the C-suite, or other departments in the organisation. Survey responses indicate that, in 2023, IT decisions are made organisation-wide and are no longer restricted to just the IT department.

Data breaches

There have been many high-profile cybersecurity breaches in both Australia and New Zealand in the past 12 months. Overall, 78% of research participants were aware of the major cybersecurity breaches, but there is a difference by country. In Australia, 83% of research participants were aware of major breaches. However, only 53% in New Zealand were cognisant of the same.

Are you aware of recent major cybersecurity breaches in [Australia / New Zealand]?



Individuals and the organisations that they work in, display alignment in the level of concern about cybersecurity breaches. Yet, only 56% of organisations have modified their cybersecurity practices, despite being apprised of the breaches. Slightly more than one-quarter (26%), have not modified their practices and 17% 'don't know' if practices have been changed. Nonetheless, there appears to be a high level of complacency in organisations in the face of major breaches.

When practices have been changed, the top four changes are:

Increasing training and awareness:

63%

Increasing firewall protection:

53%

Implementing multifactor authentication:

52%

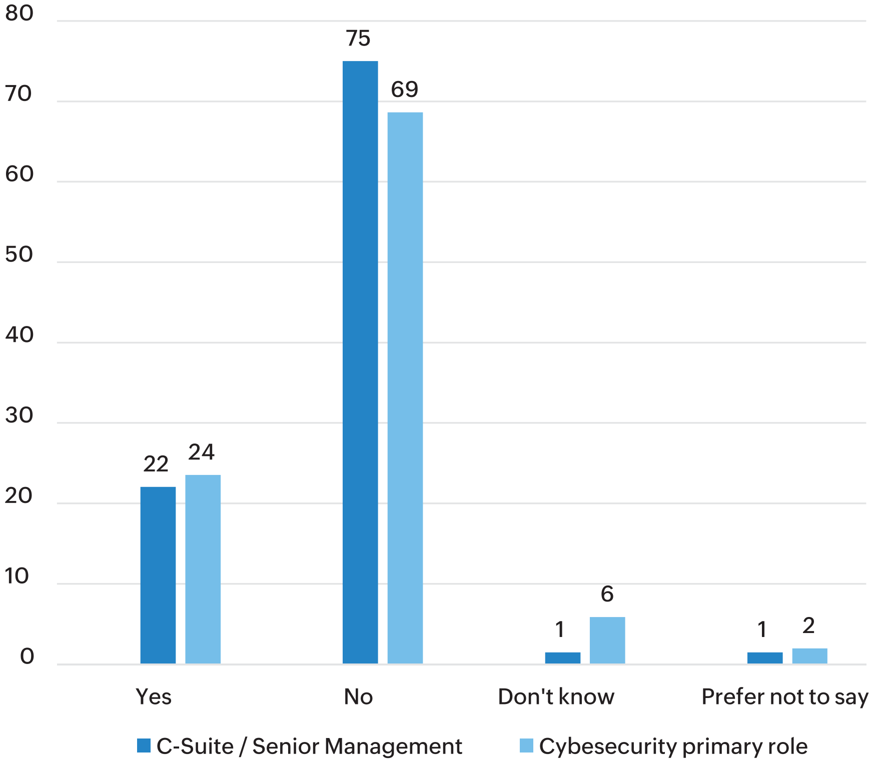
Increasing level of encryption:

49%

How have your organisations practices changed?	
Increased employee training and awareness	63%
Increased firewall protection	53%
Implemented multi-factor authentication	52%
Increased level of encryption	49%
Carried out independent cybersecurity audit	40%
Increased threat detection	40%
Checked database integrity and application security	39%
Hardening of network-plug and closing operating system gaps	34%
Implemented SSL at the appropriate levels of the network	22%
Increased frequency of red team activity and simulated attacks	20%
Used white-hat hacker to test cybersecurity	19%

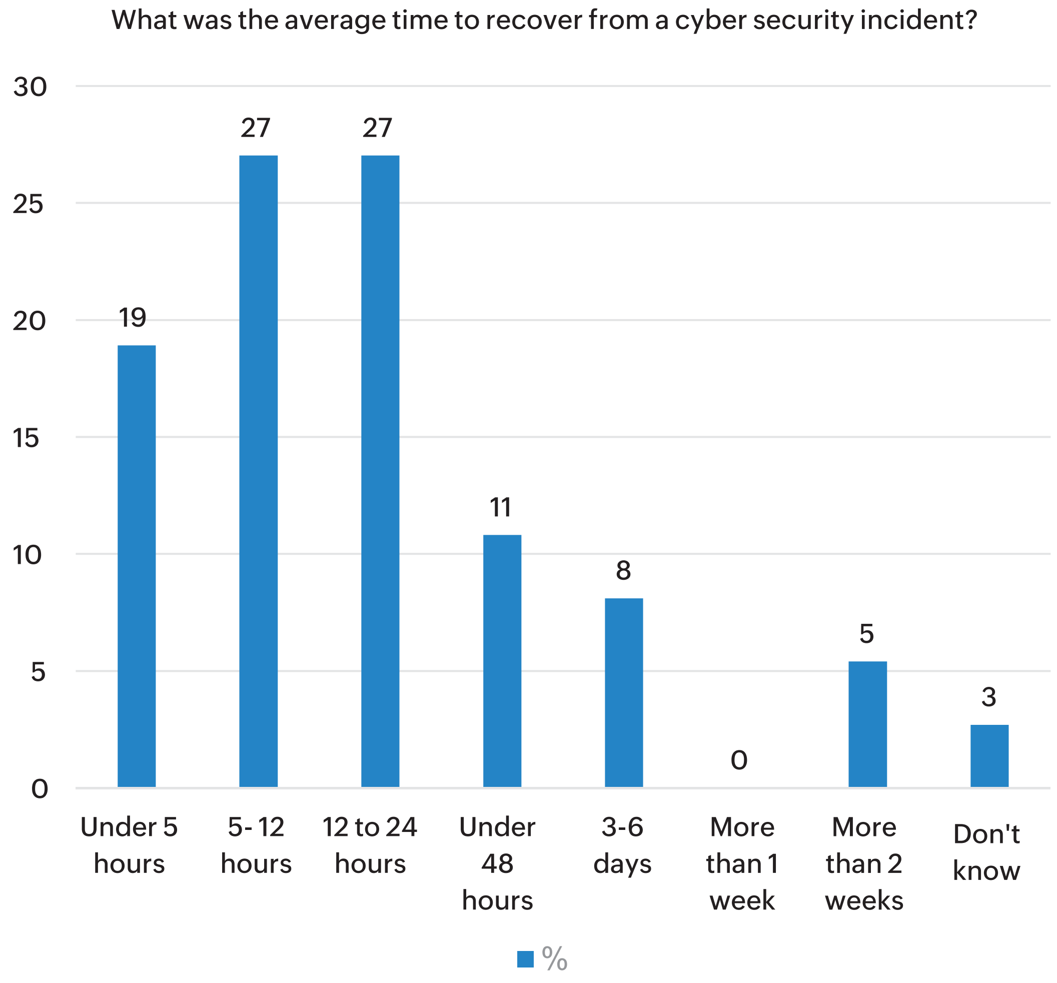
Cybersecurity breaches in the last 12 months

Just over one-in-ten (12%) have experienced a cybersecurity breach in the last 12 months. However, the real incidence is probably much higher as C-suite/senior management (22%) and those with cybersecurity as their primary role (24%) are likely to say their organisation has experienced a breach.



Has your organisation experienced any cybersecurity breach in the last 12 months?

The severity of breaches is described as 'moderate' for 41% and 'high' for 16%. The positive finding from this is that almost three-quarters (73%) were able to recover in 24 hours or less.



Data retention: Management of PII

What is PII?

PII is defined in this report as personally identifiable information that may include an individual's name, signature, address, phone number, date of birth, or other data that can identify them specifically. Recent high profile cybersecurity breaches have all involved PII.

In the research, 58% of participants commented on how their organisation manages PII. Of these respondents, just over half (57%) reviewed how their organisation managed PII in the last 12 months, with 63% being motivated by recent major data breaches. Almost three-quarters (72%) of the respondents acknowledged making changes to their PII management policies as a result, while 54% of the respondents said this has not changed at their organisation, or that they don’t know if it’s changed.

A review is the catalyst for changes in the management of PII. But data shows that many organisations have failed to carry out such reviews. Taking into account organisations that have not carried out a review, in total, only 41% have made changes to the way PII is managed in their organisation.

Where changes have been made, measures implemented include:

Reviewing access control:

56%

Revisiting the data retention policy:

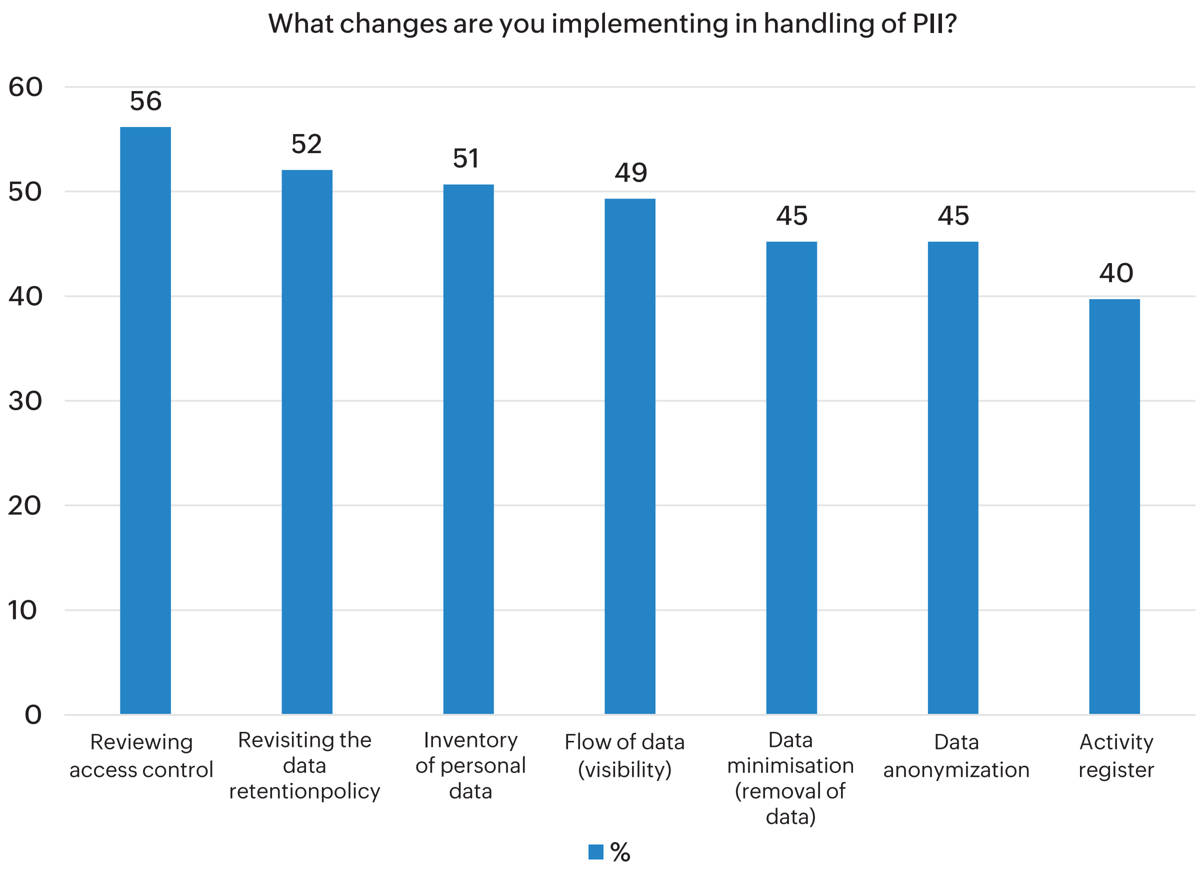
52%

Inventory of personal data:

51%

Flow of data (visibility):

49%

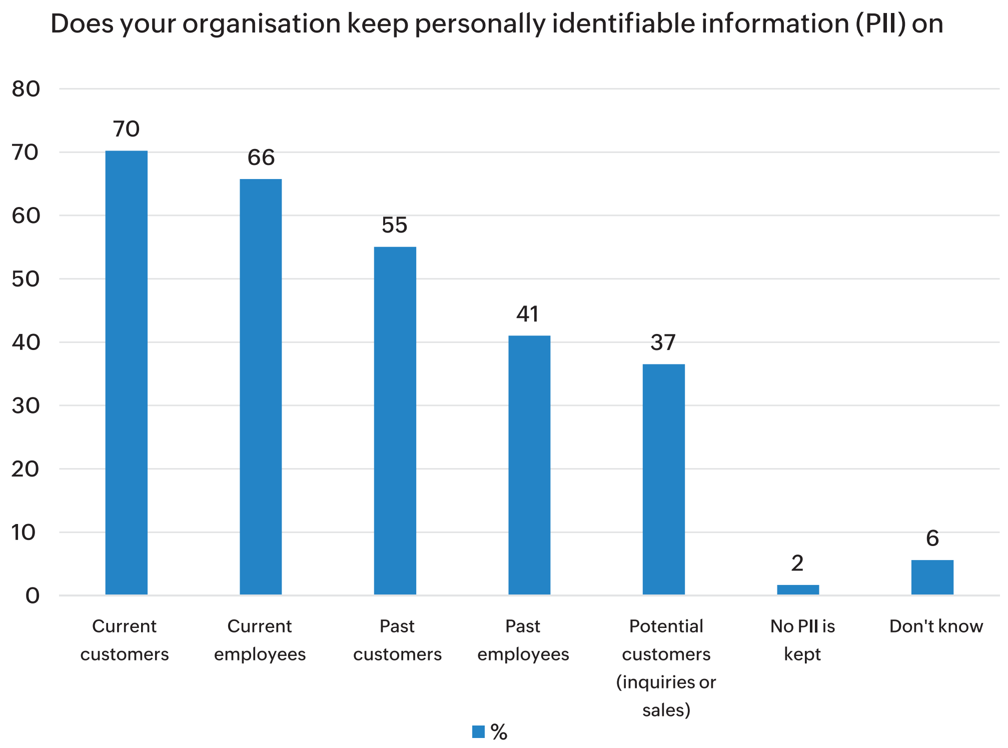


The biggest concern about PII breaches relates to malware attacks as cited by 64% of the respondents. Although this is much higher than other areas, apprehensions also rise for software supply chain vulnerabilities (44%), social engineering attacks (42%) and man-in-the-middle attacks (34%).

PII is the lifeblood of marketing and management for organisations, but also a honeypot for malicious actors.

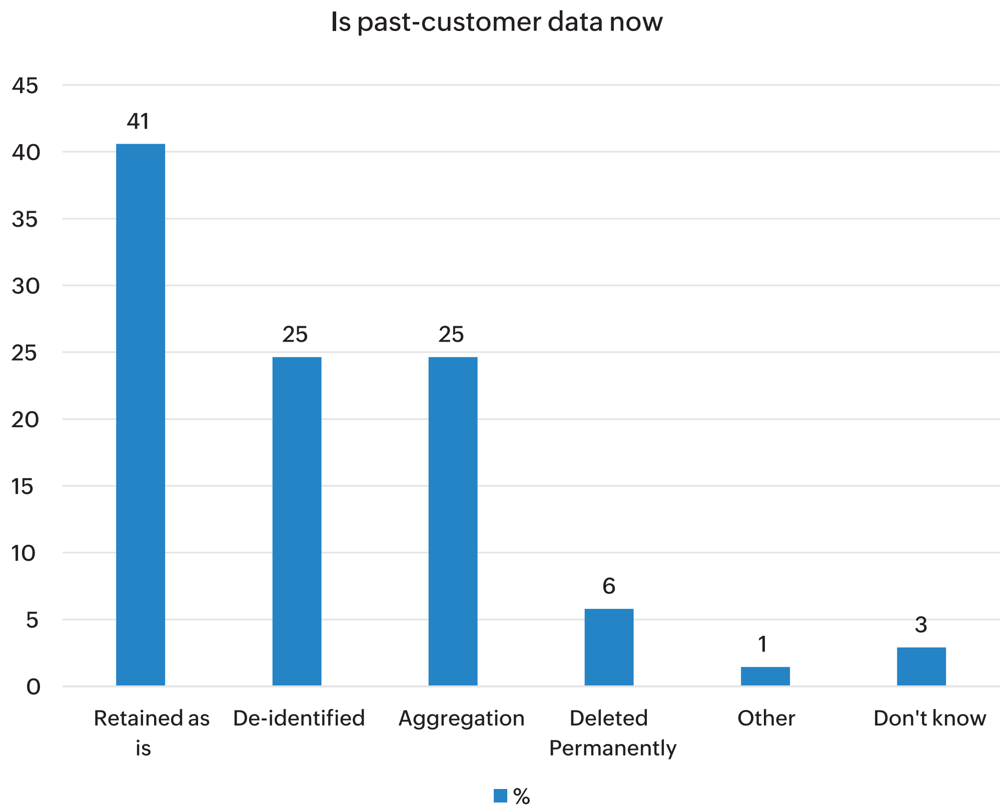
According to results from our survey, PII retained in organisations includes:

Current customers	Current employees	Past customers	Past employees	Potential customers (enquiries and sales)
70%	66%	55%	41%	37%

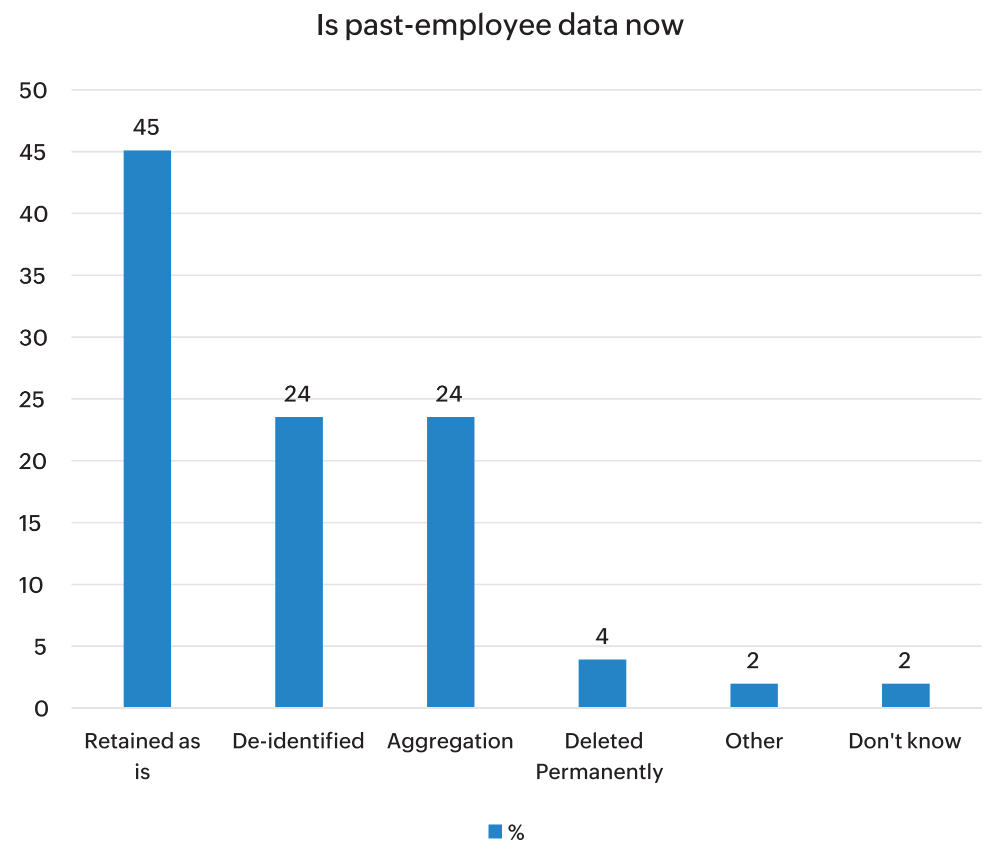


The above numbers suggest that, for obvious reasons, the most retained PII is that of the current customers and staff. The survey responses also indicate a questionable practice of organisations retaining PII of past customers and employees.

In the case of past customer data being held, one-in-five (21%) have not considered whether this data should be retained. In the survey, 70% of research participants had considered the need for past customer PII retention, but of this group 41% had retained past customer PII ‘as is’. It could be that the data was determined to be safely held. Only 25% de-identified the PII and 25% also aggregated the data.



A similar situation exists for organisations that have retained PII on past employees. Just 12% have not considered the need for retention, and 18% don't know if the need for retention has been considered or not. Of the 70% that have considered the need for retention of past employee PII, just under half (45%) have kept the data 'as is'. Only 24% have de-identified the data and 24% have aggregated the data.



Of the 12% of organisations where cybersecurity breaches have taken place in the last 12 months, just over half (51%) have involved PII. Almost two-thirds (61%) of organisations where the research participant can comment on PII, report that only 61% are equipped to handle malware attacks on PII. This means that almost two-in-five (39%) are not confident in handling the most common and damaging type of attack on PII.

From the above statistics, de-identification and aggregation seem to be the most opted for managing PII. This observation raises a valid question: Are organisations addicted to retaining PII in spite of little reason and poor general management?

Work from home

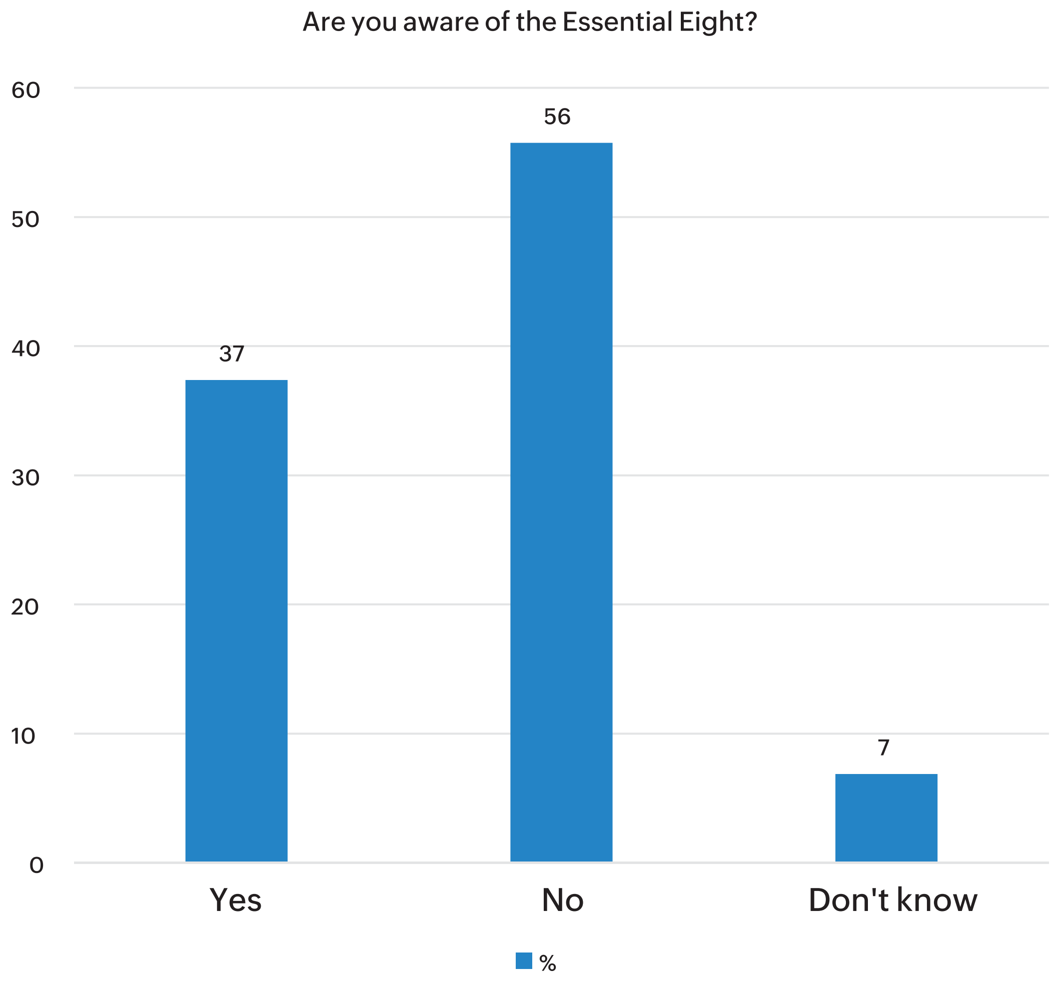
Hybrid working is the 'new normal' with 73% of organisations having their staff work remotely for some of the time, and 8% work remotely for 'all of the time'. In total, this indicates that 81% of organisations having remote workers. Three-quarters of ITDMs feel that remote working creates a more challenging security environment. Their biggest concern is risks from personal devices used for work, or work devices used for personal use (60%), followed closely by unsecured Wi-Fi networks (58%).

Which of these are concerns you have about cybersecurity and employees working from home or from anywhere?

Risks due to personal devices and personal use of corporate devices	60%	Unencrypted/unsecured way of file sharing	25%
Unsecured Wi-Fi networks	58%	Expanded attack surface	23%
Phishing attacks	41%	Diluting security controls for getting the work done	19%
Weaker security controls on remote users	34%	Dilution of access control	17%
Security awareness training relevant to remote work related risks not given	27%	None of these	4%
Inadequate Remote work policy	26%	Other	0%
Weak networks and perimeter security	26%		

Essential Eight

Given that the Essential Eight has been in common use for a while now, it is surprising that only 37% of research participants are aware of the concept. A surprising 63% of respondents said they are not aware of, or don't know about, the Essential Eight framework. Even those in senior management/C-suite (57%), and those with cybersecurity as their primary role (57%) have relatively low awareness. Of those that are aware of the Essential Eight, 83% have compliance as a requirement for IT suppliers and 71% have implemented the Essential Eight in their organisation.

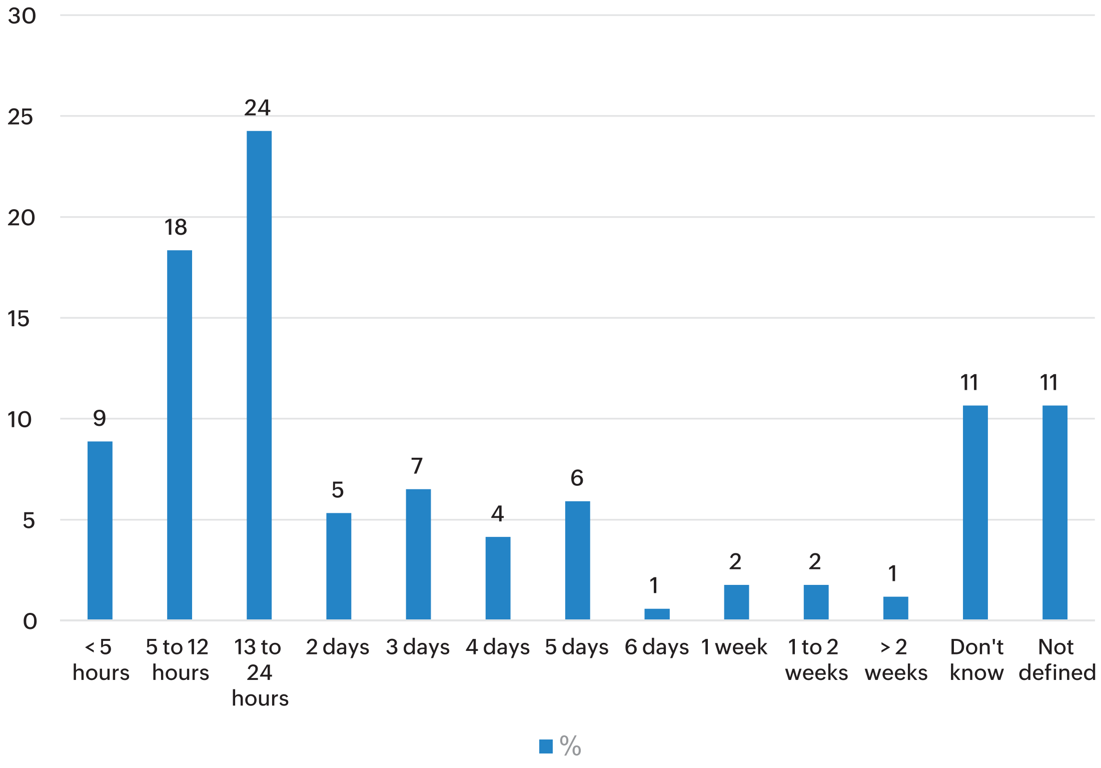


Cyber resilience

The research shows there is a huge shortfall in the level of cyber resilience policy implementation. Almost one-quarter (24%) either do not have a cyber resilience policy (15%) or don't know if there is a policy (9%). 82% of respondents whose specific role is cybersecurity were aware of cyber resilience, and of this group 88% said their organisation has a cyber resilience policy.

Of the 76% of organisations who have a cyber resilience policy, 51% define 'return to normal' as 24 hours or less. In one of the positive points of the research, where breaches have occurred in organisations, 73% were able to return to normal within 24 hours. Those 'with a plan' also test recovery frequently, with 90% testing recovering time within the last 12 months.

How long is 'return to normal' defined in hours/days in your cyber resilience plan/strategy?

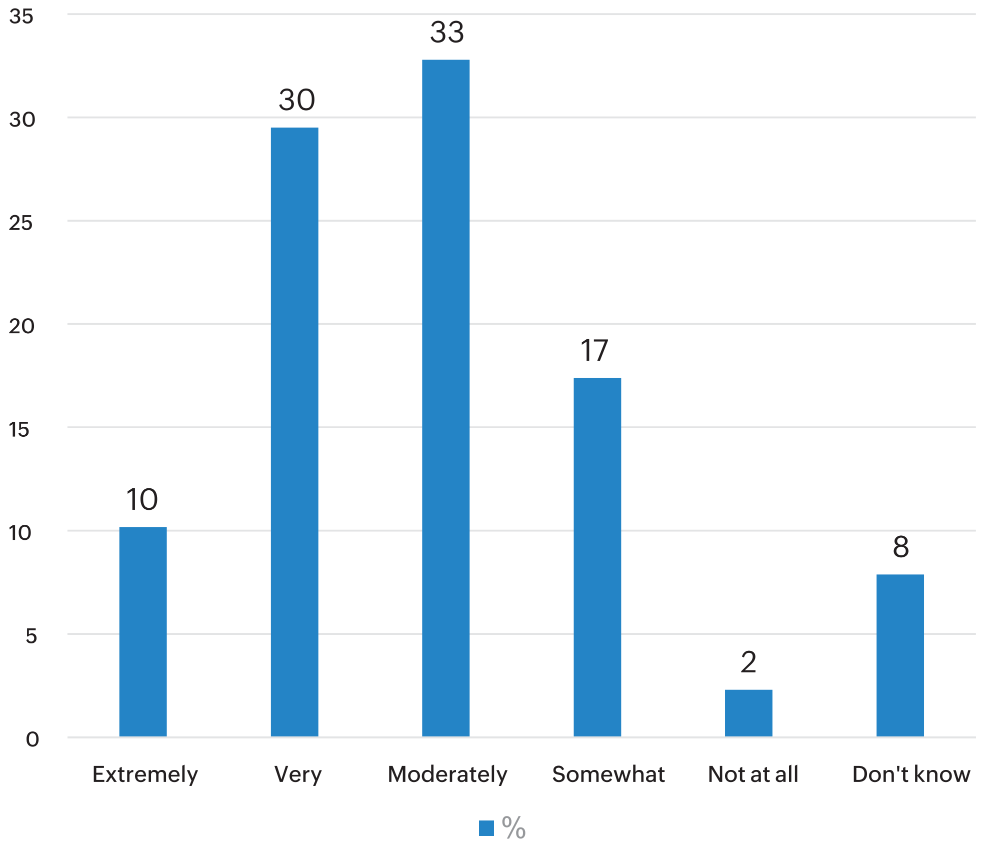


As with other findings in the report, organisations are split into those that have tested and implemented this best practice, and those that are unaware of the common threats in 2023.

Malware and ransomware

Only 40% of organisations are ‘extremely confident‘ (10%) or ‘very confident’ (30%) they can recover from ransomware without paying a ransom. This low level of confidence is reflected in the 10% who admit their organisation has paid a ransom at some time. Despite this low confidence in recovery without paying a ransom, confidence in staff is high, with 83% believing staff are either ‘very good’ (17%) or ‘good’ (66%) at identifying malware/phishing attempts.

If your business was impacted by ransomware, how confident are you in the organisation’s ability to recover without paying a ransom?



Conclusion

In light of the recent high-profile breaches, this survey has tested the knowledge and readiness of ANZ organisations with regards to cyber resiliency and security. Responses from the research participants determined these findings:

- Most organisations show complacency in cybersecurity, undeterred by their lack of knowledge about the required best practices.
- The cybersecurity breaches that are recorded might, inadvertently, understate the damaging effects it can have on an organisation.
- Organisations recognising the importance of PII best practices has spurred the need for proper retention and management measures.
- Concerns linger around cybersecurity in the wake of the hybrid-working model, that can serve as an attack surface for cyberattacks.
- Although the Essential Eight is an established concept, many organisations are unaware of the framework, or that it should be immediately implemented to safeguard their IT infrastructure.
- Many organisations have an inadequate cyber resilience policy that translates into low confidence in ransomware recovery.
- This report about the state of cyber resilience in ANZ can serve as the starting point for achieving a cyber secure organisation.

Methodology

This report, based on the study titled 'How cyber resilient are organisations in ANZ?', was conducted by Sydney-based research and insights advisory StollzNow, and commissioned by ManageEngine. This study followed an online panel, self-complete methodology. The research participants were independently selected by the online permission- based research panel supplier Pureprofile. Research participants received an incentive for completing the survey. Quotas were set for Australia (250) and New Zealand (50). Interviewing commenced August 1, 2023 when 58 questions were asked, and a total of 306 fully completed surveys were received.

ManageEngine

www.manageengine.com

me-pr@manageengine.com