



**AUCLOUD**



# **Sovereign Cloud Holdings Limited**

**Investing in Australia's Cyber Security**  
**SOV Update & Industry Panel**

17 June 2024



# Peter Maloney

CEO, AUCloud







# AUCloud (SOV) Update



# Our Vision and Strategy



## Our vision

To become **Australia's preferred partner to Government & Enterprise in cloud, data protection & cyber security**

## Our strategy

Build, partner or acquire capabilities to create a **diversified cyber security and cloud solutions business** with a national footprint, at scale

## Delivered through

### Strategic Objectives

Integration of Acquisitions | Customer Growth | Partnerships | Expand Offerings

## Enabled by

**Full-service secure cloud, MSP & cyber security provider** at scale



Sovereign Cloud Infrastructure



Managed Cyber Security



Managed IT Services

## Solutions

## Capabilities and Opportunities



### Sovereign Cloud Infrastructure

- ✓ Secure sovereign cloud infrastructure which hosts Enterprise, Federal, State & Local Government customer's applications and data at scale
- ✓ Cloud zones located across Sydney, Melbourne, Brisbane & Canberra
- ✓ Security accreditations: Certified Strategic and IRAP assessed Protected under the CAAF, ISO 27001 and member of DISP



### Managed Cyber Security

- ✓ 24/7 monitoring, governance, risk and compliance strategies, auditing a customer's security posture or testing a customer's ability to react to a cybercrime
- ✓ Operates on the front line to detect cyber-crime with Security Operations Centre service protecting some of Australia's best-known brands with the latest detection and response services



### Managed IT Services

- ✓ Day-to-day management of customers' Cloud and On-Premises infrastructure and environments
- ✓ Enterprise Managed Services, Data Protection & Backup Solutions
- ✓ Signed Premier Partner Agreement with Broadcom by VMWare, protecting AUCloud's existing position and opening up a new channel to resell VMWare licences to other MSPs

**Full-service secure cloud, MSP & cyber security provider**

# AUCloud Today



## Broad Product Portfolio

**Broad product portfolio** aligned to customer needs, with revenue spread across the broad spectrum of cyber security and cloud solutions

## Expanded Customer Base

Combined **200 customers bring scale and diversified revenue** across local, state and federal Government agencies, mining, finance, professional services, education, health and distribution sectors

## National Footprint

Strengthening cyber security position with the platform to create **a cyber security national footprint**

## Improved Partner Network

**Expanded partner network** will include AWS, CISCO, Commvault, Google, Microsoft, NetApp, Pure Storage, Rubrik, VMware, Veeam which when combined delivers cutting edge technology and expertise

## Experienced Leadership

**Highly skilled team, with** continuous investment in uplifting skills, capabilities & know-how

## Key AUCloud Metrics<sup>1</sup>



Customers #  
**200+**



ARR  
**\$22m**



% ARR  
**88%**



ARPU  
**\$173,000**



Team  
**115**

<sup>1</sup>. Key metrics are as at 31 May 2024.



# Acquisitions Overview



AUCloud completed 3 strategic Acquisitions in early May 2024.

- **PCG Cyber** is a Canberra based cybersecurity consultancy firm specialising in Australian Government security advice and operations
- **Venn IT** Venn IT is a Queensland and South Australia based MSP and professional consulting business, data resilience & backup protection specialist servicing customers in the mining, financial services, education, and distribution sectors
- **Arado** is a suite of cloud and managed services, with a strong presence in Queensland. Arado has a customer base in State & Local Government and enterprises accounts across various sectors, including agriculture, industrial, health and resources




## Strategic Rationale

- 1 Three acquisitions create a platform for a scaled enterprise in a fragmented cloud and cyber security sector. Targeting strong business economics at customer and margin level & continued M&A to scale up quickly through further waves of accretive acquisitions to absorb high-quality cyber businesses
- 2 All acquisitions are independently profitable in 1H FY24, have a diversified customer base with predictable revenue and CAPEX light business models. Post completion MergeCo will have ~84% Annual Recurring Revenue (ARR<sup>1</sup>)
- 3 Acquisitions leverage capital deployed in sovereign cloud infrastructure increasing utilisation of the built capacity, along with revenue, product & geographic diversification spanning cyber security and secure cloud solutions to increase competitiveness
- 4 Corporate Australia and Government entities continue to focus on strengthening their cloud and cyber security posture, with >60% Australian companies expected to increase cyber budgets in 2023<sup>2</sup>

1. As at December 2023 on a pro forma MergeCo basis. Refer to Appendix G (Glossary) for definition for definition of ARR and ARPU. 2. Source: "Rising demand for cyber security creates investment opportunities" <https://www.austrade.gov.au/en/news-and-analysis/analysis/australias-a-7-billion-cyber-security-opportunity>

# Integration of recent Acquisitions

Integration progressing to plan and the recently acquired businesses are seeing the benefit from synergies and scale; including cross sell opportunities.

Acquired Business	People	System	Process	Brand
	Partial Integrated / 25 people	Partial Integrated	Partial Integrated	Partially Integrated
	Partial Integrated / 16 people	Partial Integrated	Partial Integrated	Partially Integrated
	Partial Integrated / 26 people	Partial Integrated	Partial Integrated	Completed Now AUCloud

## Key steps undertaken

- A new Leadership Team structure has been created to align with key revenue divisions of Cyber Security, Cloud and Managed Services
- Implemented headcount reductions generating annualised savings of approximately \$7.3M
- Financial Systems integrated for consolidation reporting
- Rebranding to AUCloud & AUCyber commenced

## Next steps to achieve full integration

- Consolidation of data centre infrastructure
- Rationalise office locations in Brisbane & Canberra
- Focus on sales & marketing to accelerate cross-sell opportunities to existing customers & build the consolidated pipeline
- Office technology consolidation
  - Collapse onto aucloud.com.au domain
  - Customer interface (ITSM) application consolidation

# Overview of MergeCo

## Impact of Acquisitions

## Pro Forma Financial and Operating Profile

- ✓ Revenue, product & geographic diversification spanning cyber security and secure cloud solutions to increase competitiveness
- ✓ Expanded customer base with predictable Annual Recurring Revenue
- ✓ Increased ARPU via fully integrated model of product bundling
- ✓ Acquisitions leverage capital deployed in sovereign cloud infrastructure

Metrics (\$m)	FY23A Stat. AUCloud	FY24F Stat. AUCloud <sup>1</sup>	FY24F Pro forma MergeCo <sup>1</sup>	FY25F Stat. MergeCo <sup>1</sup>
Revenue	6.5 <sup>2</sup>	10.9	28.9	36.6
Gross Margin %	n/m	36%	68%	70%
<b>Underlying EBITDA<sup>3</sup></b>	<b>(15.7)</b>	<b>(10.1)</b>	<b>(2.0)</b>	<b>4.7</b>
Depreciation-ROU Assets <sup>4</sup>	(1.5)	(1.4)	(1.4)	(1.6)
Depreciation-Other Assets <sup>4</sup>	(3.9)	(4.2)	(4.2)	(4.0)
EBIT	(21.1)	(15.7)	(7.6)	(0.9)

1. FY24 Forecast (Stat. AUCloud) represents 6 months' actual results + 4 months' forecast of AUCloud standalone, + 2 months' synergised forecast on a MergeCo basis (assuming the Acquisitions occur on 30 April 2024); FY24F Pro forma represents aggregated MergeCo financials as if the Acquisitions occurred on 1 July 2023; FY25F is based on forecast on a MergeCo basis. See Appendix A for basis of preparation and key assumptions. 2. FY23A revenue of \$6.5m includes \$2.1m of non-recurring Technical Project Services related revenue, and \$4.4m of cloud and cyber security services revenue. Refer appendix g Glossary for definition of ARR and ARPU. 3. Excludes one-off acquisition and restructuring costs of \$1.3m and the impact of Share Based Payments – refer to Note 6 on Page 13. 4. Depreciation of Right-Of-Use assets relate to data centre costs and rental costs (cash items). Depreciation of other assets relates to non-cash items. 5. Key metrics are indicative as at December 2023, and post synergies on a pro forma basis.





# Cyber Security Landscape

**Australia** is the world's 4<sup>th</sup>  
biggest victim of cyber-  
crime...

# Why does it matter to Australia?

Protection of Intellectual Property

Brand equity & reputation

Business continuity

Regulatory and legal obligations

The eco-system is large & complex





## HWL Ebsworth hack affected government departments, cyber security coordinator says

By political reporter Matthew Doran  
Posted Wed 5 Jul 2023 at 6:50pm



Home / SME Law

## cyber security, says report

SHARE

Data and computer security

## Australian law firm HWL Ebsworth hit by Russian-linked ransomware attack

— Exclusive

## 'Big game hunting' hackers claim major breach of law firm HWL Ebsworth

CYBER SECURITY NEWS · 3 MIN READ

## Data Breach at Australian Law Firm That Caters to Government Agencies, Finance Institutions Could Be the Worst in National History

SCOTT IKEDA · JUNE 28, 2023



Australia has been experiencing unusually serious problems with data breaches that involve mass amounts of sensitive information for nearly a year now. It had

## WA government insurance claim data potentially stolen by ransomware gang AlphV in law firm hack



**CYBER SECURITY NEWS · 3 MIN READ**

# Data Breach at Australian Law Firm That Caters to Government Agencies, Finance Institutions Could Be the Worst in National History

SCOTT IKEDA · JUNE 28, 2023

### HWL Ebsworth hack affected government departments, cyber security coordinator says

Australia's new cyber security coordinator has confirmed multiple government departments and agencies have been affected by the massive HWL...

5 July 2023

### HWL Ebsworth hack: Queensland says its files were taken after criminals release Victorian documents

State's chief information security officer says information from Victorian departments and agencies was accessed.

1 month ago

### Tasmania gov caught up in HWL Ebsworth breach

The Tasmanian government is exposed to the data breach of law firm HWL Ebsworth, and was notified of that exposure by federal authorities...

9 June 2023

### Tasmanian government reports possible data breach linked to alleged HWL Ebsworth hack

The Tasmanian government is reporting that the Commonwealth has been in touch regarding a possible leak of state government data on the dark...

14 June 2023

### 'They want to instil fear': Victorians' files bound for dark web after data breach

Credit card details, driver's licences and birth certificates could be among the personal information of Victorians that could be published...

1 month ago

### Legal documents from the Victorian Government published on dark web

Legal documents from the Victorian Government have been released to cyber criminals on the dark web after ...

1 month ago

### Data leak at major law firm sets Australia's government and



# Cybercrime is growing in Australia

- The volume of Cybercrime reports YOY are **up 23%**
- Average cost of Cybercrime reported YOY are **up 14%**
- Calls to the Australian Cyber Security Hotline YOY are **up 32%**
- On average, a Cybercrime is reported **every 6 minutes**
- Ransomware alone causes **\$3 billion in damages** to the Australian economy every year
- Top 3 Cybercrime types for businesses:
  1. email compromise
  2. business email compromise (BEC) fraud
  3. online banking fraud
- **300,000 scams** are reported in Australia each year; at a cost to everyday Australians of **\$476 million per year**





Over **94,000** cybercrime reports in Australia >  
an increase of **23 per cent** from the previous year.

A cybercrime is reported **every 6 minutes** >  
compared to every 7 minutes last financial year.

Average loss of **\$97,200** per medium sized business.

*Source: Australian Signals Directorate (ASD), Australian Cyber Security Centre  
Annual Cyber Threat Report [July 22- June 23]*

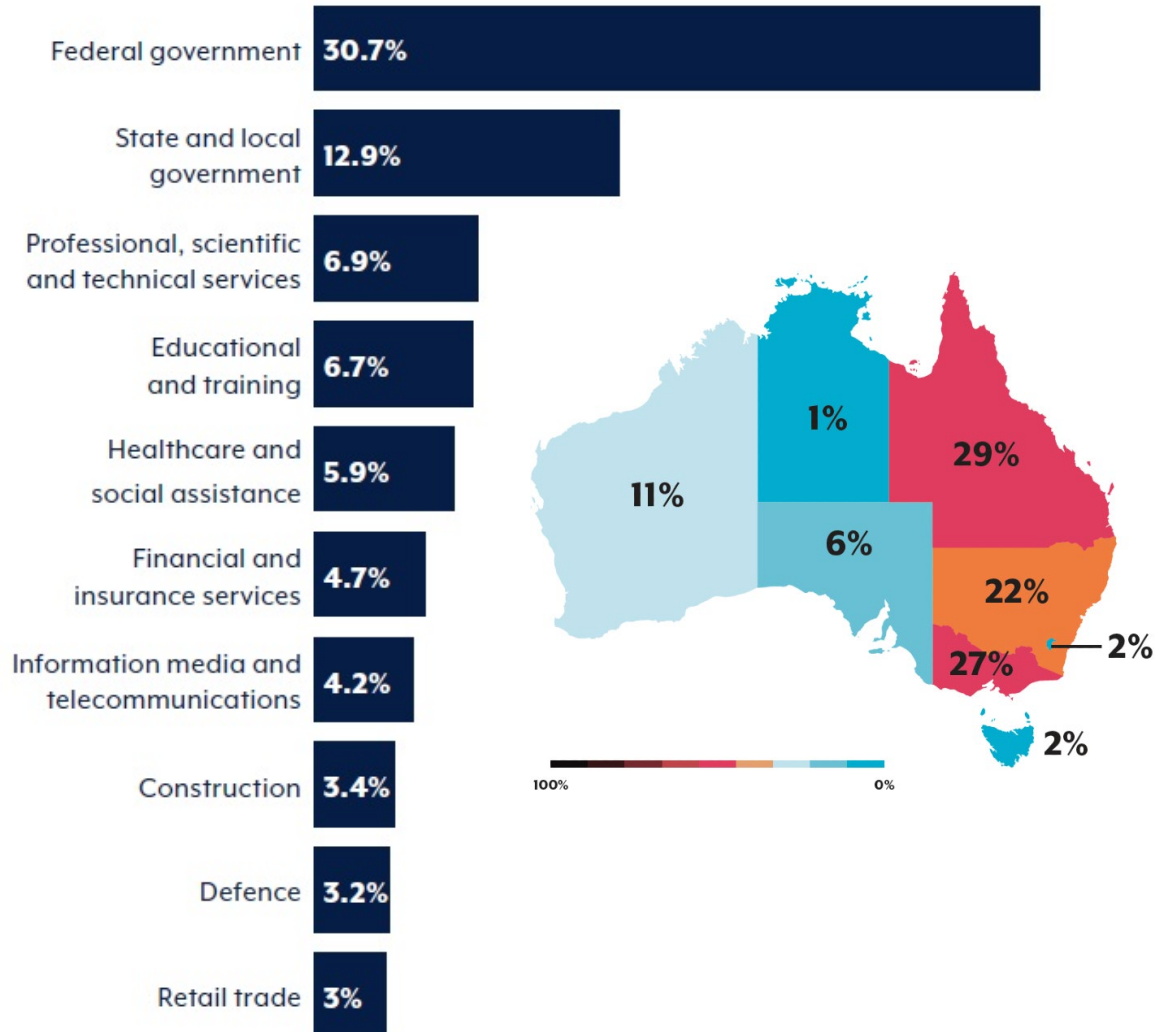


**20** Australian companies  
will suffer a cyber-attack  
during this webinar

**\$2 Million**

# Australian cyber security incidents

## Top 10 cyber incidents by sector



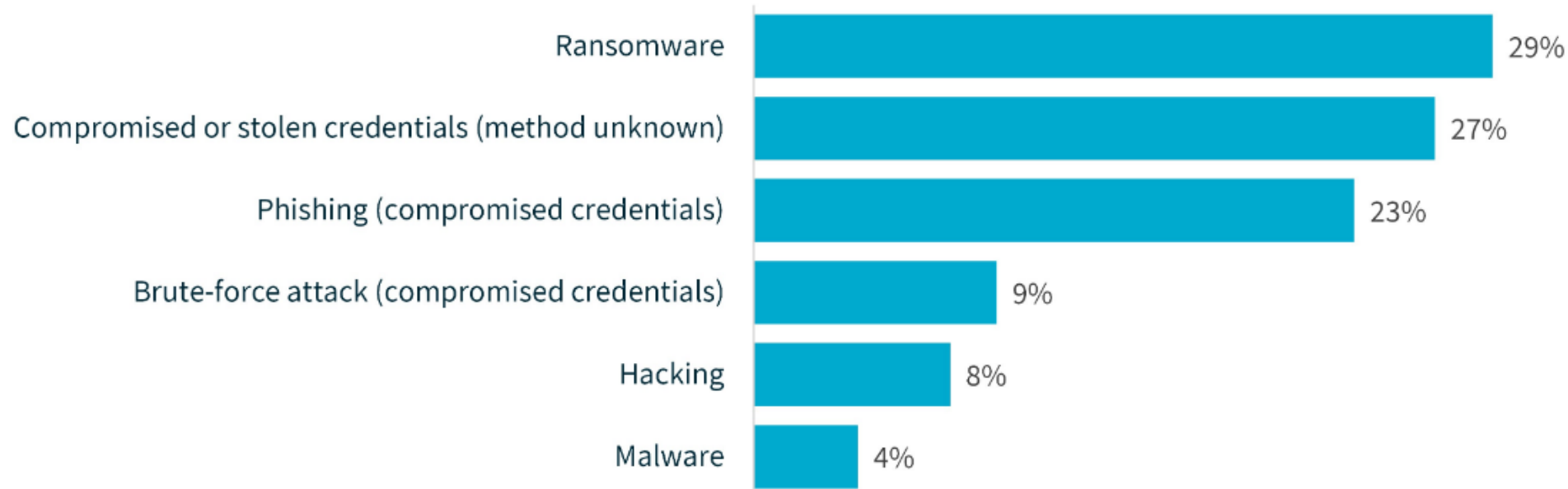
## Types of information stolen in data breaches

Contact/ Identify Information	50%
Financial Information	14%
Commercial Sensitive	10%
Other Sensitive	9%
Health Information	6%
Unknown	6%
Tax File Numbers	4%

# Key Trends: Why is Australia under attack?

**45% of all data breaches resulted from cyber security incidents  
(222 notifications)**

## Cyber incident breakdown



# Strong industry drivers in cyber security

- The Australian Government committed to being a world-leader in cyber security by 2030. This is outlined in the 2023-2030 Australian Cyber Security Strategy.  
“Stronger cyber protections will allow our citizens and businesses to prosper; it will also help them recover quickly after a cyber-attack.”
- The Australian Government is also committed to a new era of public-private partnership; this aims to improve Australia’s cyber security and resilience.

*“Cyber security touches the lives of every Australian. On average, one cybercrime is reported every 6 minutes, with ransomware alone causing up to \$3 billion in damages to the Australian economy every year.”*

## **The Hon Clare O’Neil MP**

Minister for Home Affairs and Cyber Security



## **Legislative Reforms**

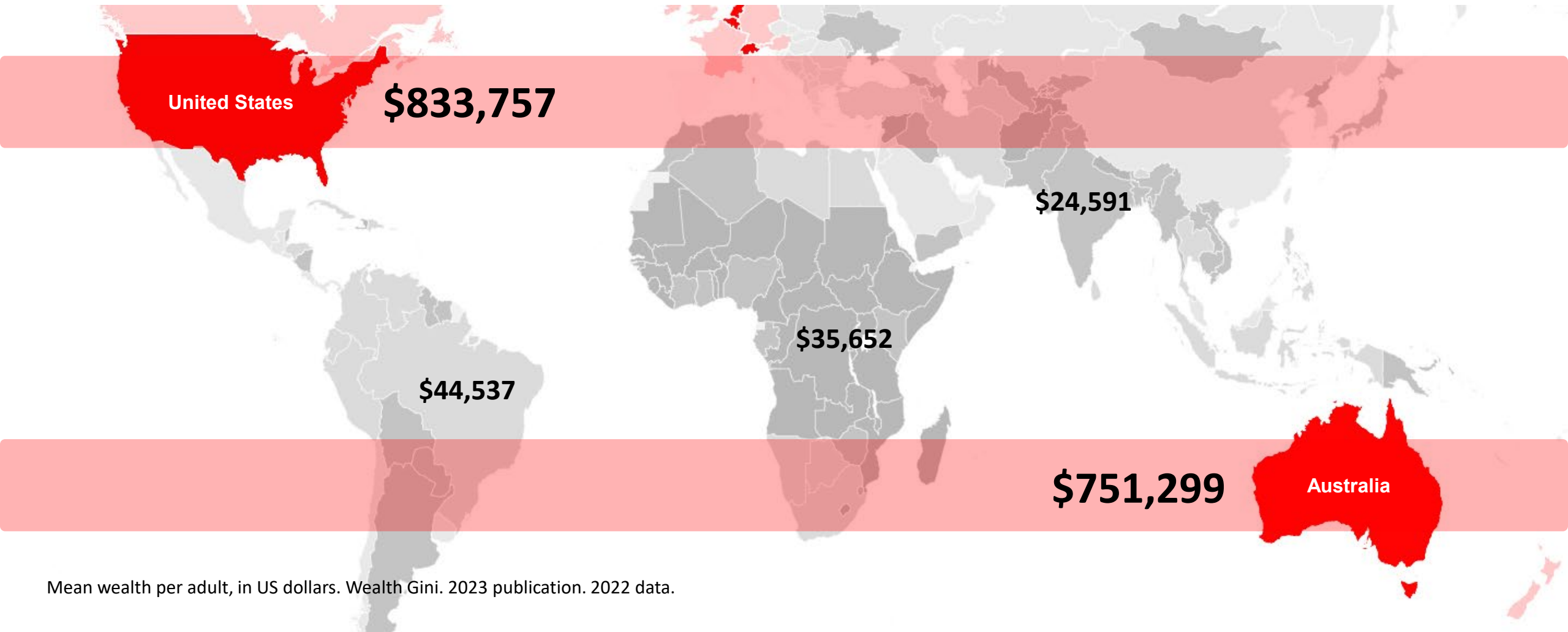
- Security of Critical Infrastructure Act 2018 (SOCI)
- The Privacy Act 1988 (Privacy Act)





**CYBERATTACK?**

# Australia's prosperity is attractive to cybercriminals



Mean wealth per adult, in US dollars. Wealth Gini. 2023 publication. 2022 data.

Internet of things

# IOT





POWER VIRUS  
TERRORISM NETWORK MISSILE CRISIS  
TECHNOLOGY ESPIONAGE  
DETONATE WAR ATTACK INTERNET  
COMMUNICATION CRIMINAL DANGER  
CONFLICT THREAT ARMY  
TERRORIST VIOLENCE KAMIKAZE BUSINESS CRIME  
ARMED  
CYBER  
WARFARE  
HACKER  
SECURITY COMPUTER  
DATA  
INFORMATION MILITARY  
SAFETY SOLDIER  
VILLAIN  
WEB  
RELIGION SOFTWARE  
CYBERWARFARE  
EXTREMIST



# Cyber Crime in the **Health sector**



# Health ranks 1<sup>st</sup> for cyber crime in Australia



Health service providers



Finance (incl. superannuation)



Insurance



Legal, accounting & management services



Recruitment agencies



Source: Australian Government - Officer of the Australian Information Commissioner. Notifiable Data Breaches Report, July to December 2022

**41%** of healthcare organisations in Australia experienced a cyber attack in 2023.

**71% of Australians  
believe the  
responsibility of  
healthcare data sits  
directly with the  
Federal Government or  
the healthcare provider.**

*Source: AUCloud 2024 Cyber Security Healthcare Report*



# Research: Australians are concerned about healthcare data

**82%**

Australians are worried about unauthorised access to personal health records.



**9/10**

Australians said health information security would affect their choice of healthcare provider.



# Cyber Crime in the Legal industry



# Law firms rank 4<sup>th</sup> for cyber crime in Australia



Health service providers



Finance (incl. superannuation)



Insurance



Legal, accounting & management services



Recruitment agencies



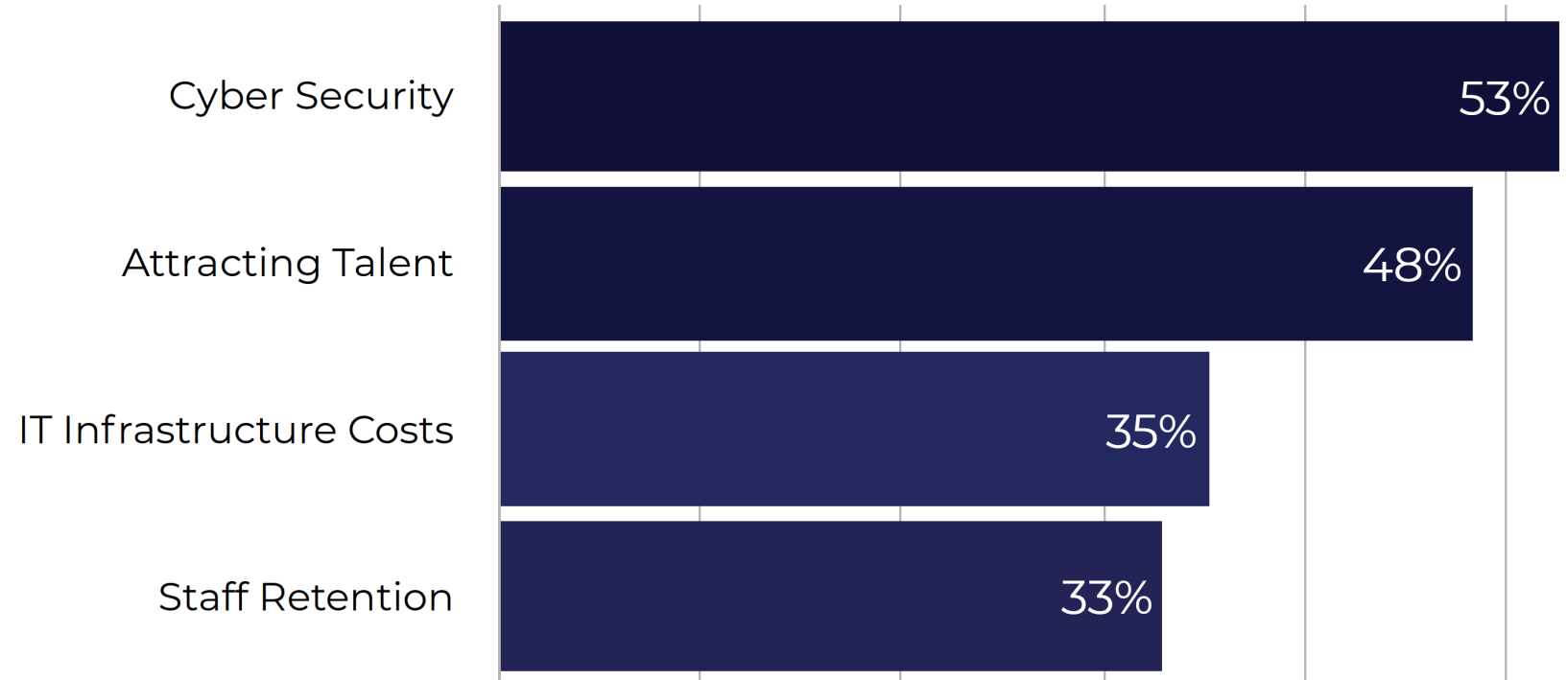
Source: Australian Government - Officer of the Australian Information Commissioner. Notifiable Data Breaches Report, July to December 2022

# Operational challenges for law firms

Cyber Security  
is the

**#1**

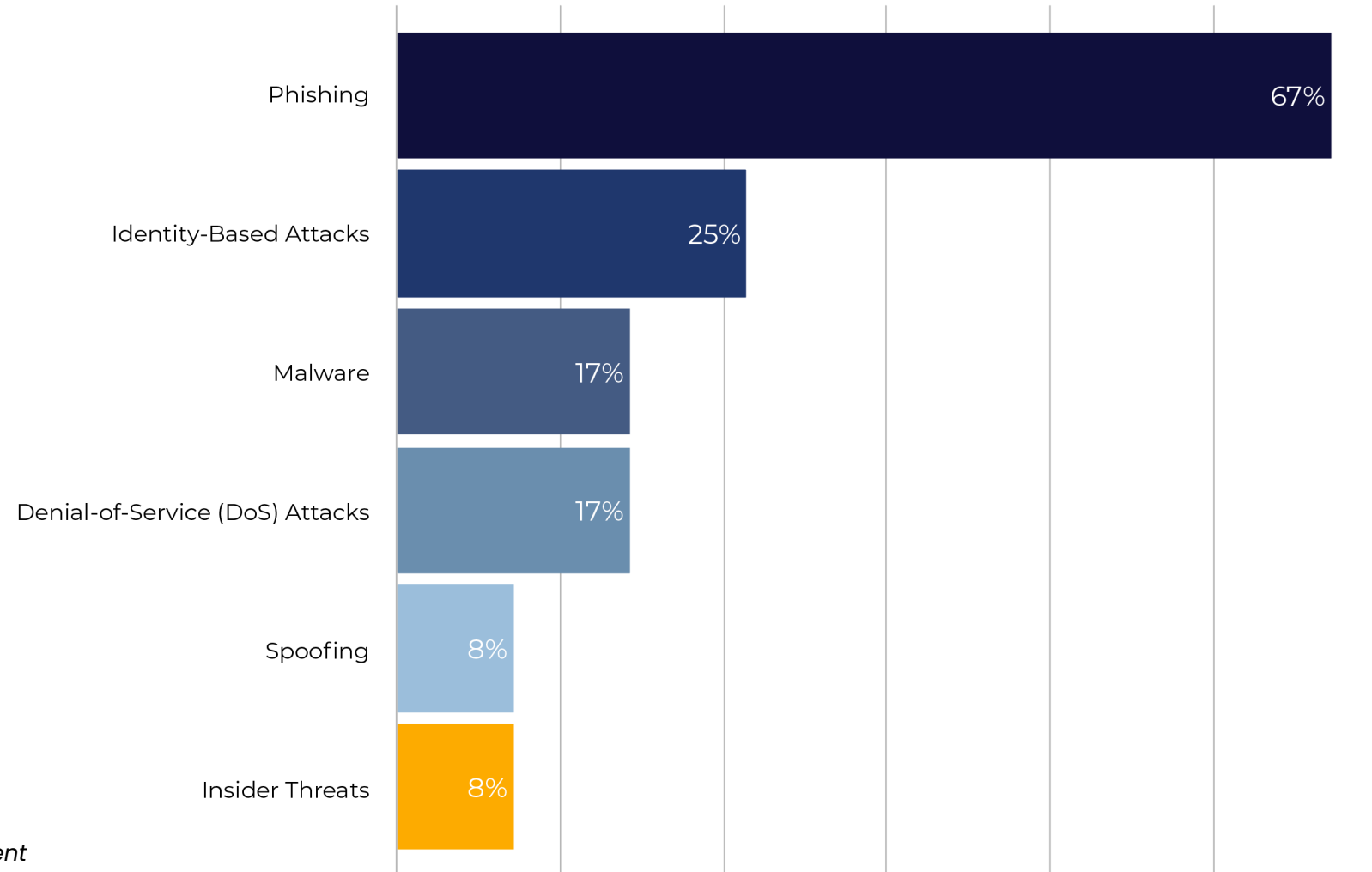
challenge  
for Australian  
law firms.



# Cyber Attacks on Australian Law

**14%**

of law firms  
experienced  
cyber-attack in the  
past year.



Source: 2023 Australasian Legal Practice Management  
Association AUCloud State of Cyber Security in Law Report

# Anything under 100% is unacceptable

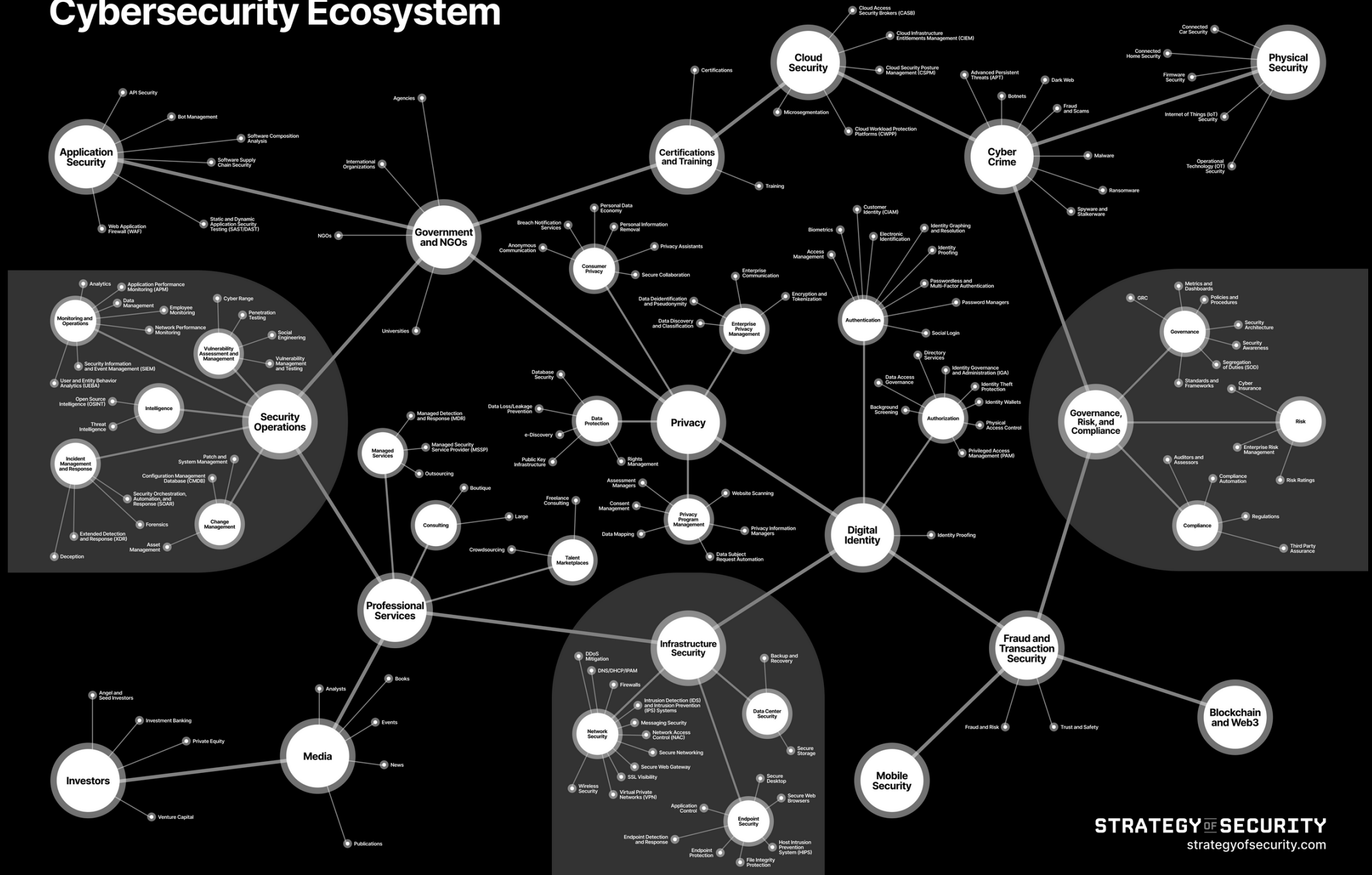
**57%**

of firms believe  
they are doing  
enough to protect  
itself against a  
cyber attack.

Cyber training	84%
Penetration testing	46%
Essential 8 awareness	53%
Business continuity plan	59%
Cyber incident plan	36%
Backups	91%



# Cybersecurity Ecosystem





# Cybersecurity Framework

**Identify**

**Recover**

**Protect**

**Respond**

**Detect**

Asset Management  
Business Environment  
Governance  
Risk Assessment  
Risk Management Strategy

Recovery Planning  
Improvements  
Communications

Access Control  
Awareness Training  
Data Security  
Information Protection  
Processes and Procedures  
Protective Technology

Anomalies and Events  
Security Continuous Monitoring  
Detection Processes

Response Planning  
Communications  
Analysis  
Mitigation  
Improvements

# Essential 8



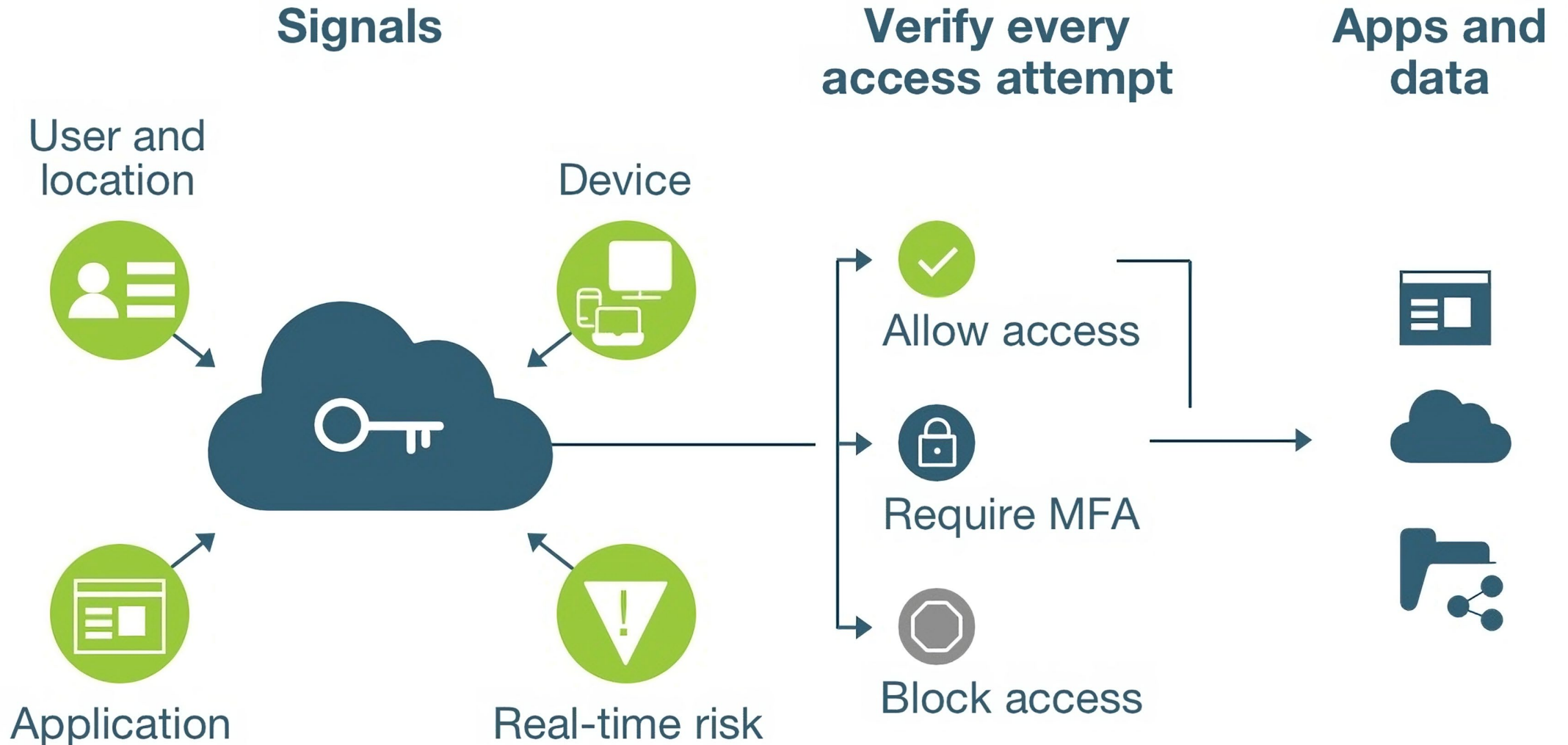


# Zero Trust Best Practices

*Low on trust, High on  
Security*



# Zero Trust Security Approach



# Protecting Australian organisations and their data



## IDENTIFY

- Security Awareness & Phishing Training
- Vulnerability Scanning
- Security Testing & Consulting
- Governance, Risk and Compliance (GRC)



## PROTECT

- Managed Detection & Response (MDR)
- Network Security Monitoring
- Endpoint Detection (EDR/XDR)
- Sovereign Cloud Services
- Backup & Recovery



## DETECT

- Managed Security Operations Centre (SOC)
- Managed Security Services
- Dark Web monitoring



## RESPOND

- Incident Response
- Digital Forensics
- Crisis Management



## RECOVER

- Backup & Recovery
- Sovereign Cloud Services





# Panel Discussion



# Cyber Security Panel



**Annie  
Haggar**

Principal, Cyber GC



**Jason  
Murrell**

Independent Chair, Cyber  
Security Certification  
Australia (CSCAU)



**Peter  
Maloney**

CEO & Managing Director,  
AUCloud



**David  
Milin**

Head of Cyber Security,  
AUCloud



**AUCLOUD**