WHITEHAWK

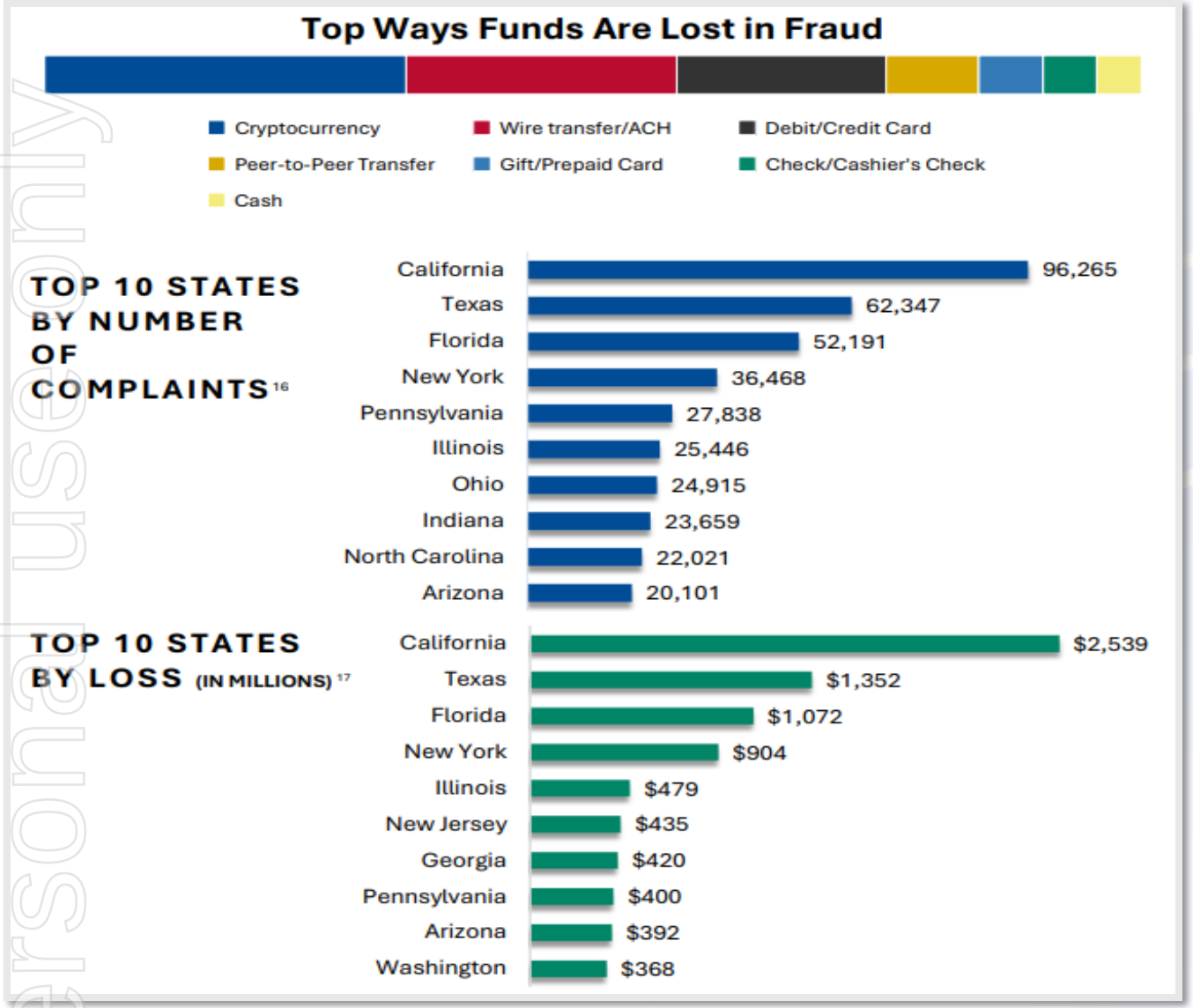
National Cyber Resilience Moonshot

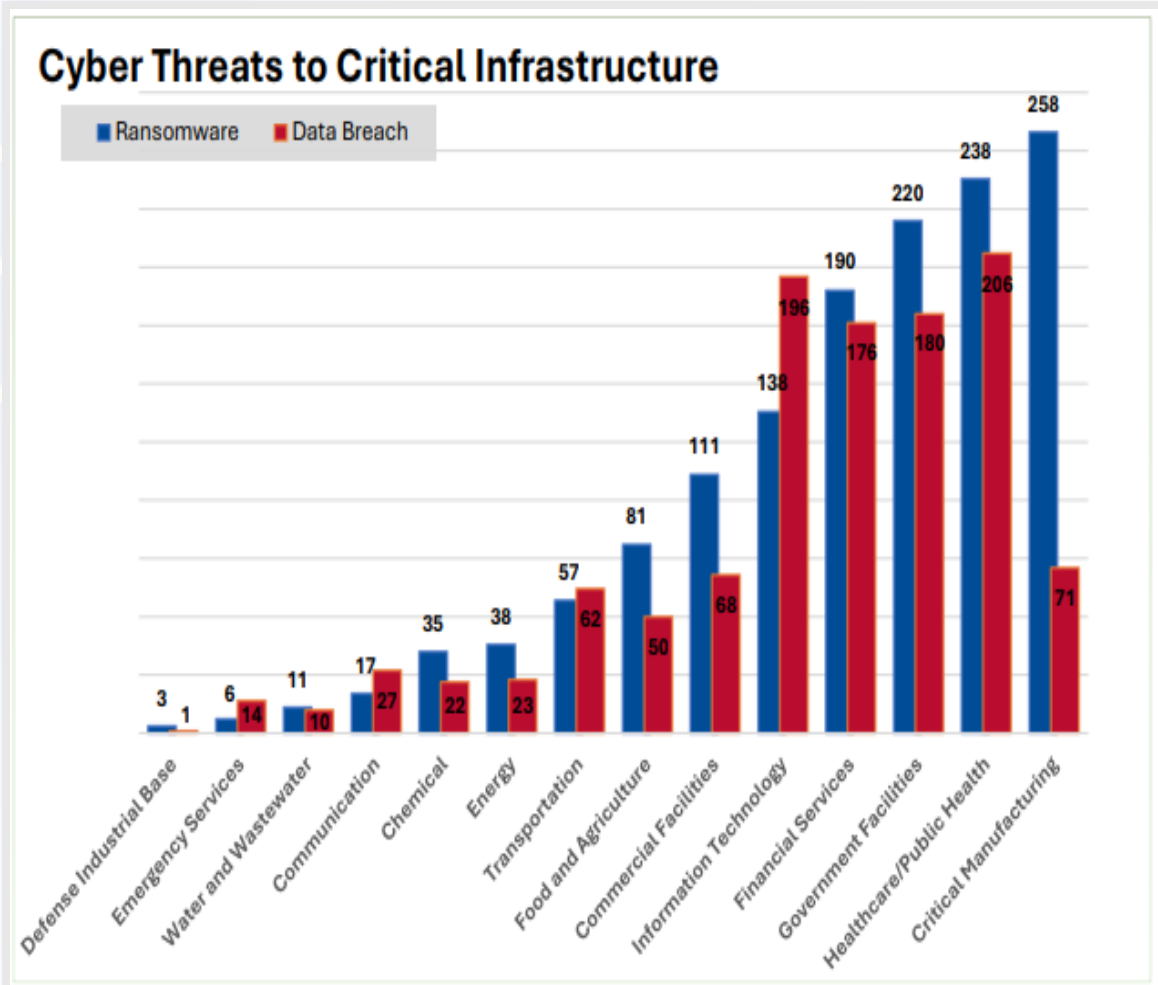
Next-Gen Globally Available Proven Datasets, Technologies, AI/ML Analytics & Automated Reporting

AGM 20MAY25

www.whitehawk.com

2024 U.S. Critical Infrastructure (CI) Threat Landscape





2024_IC3Report.pdf

Australian Cyber Key Insights

Australian Cybersecurity Industry Statistics (2024)

Economic Growth

$6.13 billion
Cyber security revenue was estimated at a value of $6.13 billion in 2024

an increase of **9.66%** in 2023

$9.99 billion
Cyber security sector generated an estimated Gross Value Added (GVA) of $9.99 billion in 2024

$348 million
Cyber security founders raised $348 million in private investment

increasing from **$105 million** in 2023

Industry Growth

302
The cyber security industry comprises of 302 Australian companies

97 per cent
of companies are Australian owned and operated

67 per cent
of cyber security companies provide cyber security products

45 per cent
Small companies (5–19 employees) comprise 45 per cent of the industry

30 per cent
Micro companies (0–4 employees) comprise 30 per cent of the industry

Workforce

137,453 people
were employed in the Australian cyber security workforce, an increase of 9.27 per cent on the previous year

- 56,080 were identified as Dedicated Roles (41 per cent) of which 20,500 (36 per cent) were identified as Core Roles
- 81,373 were identified as Related Roles (59 per cent)

25 per cent
of the cyber security workforce identify as female, an increase of 8 per cent from 2021

Forecast of 193,413 in 2029
In 2029, the workforce is forecast to rise to 193,413, representing an overall growth of 41 per cent in five years

- Dedicated Roles are forecasted to grow to 79,334, accounting for 41 per cent of the industry workforce
- Related Roles are forecasted to grow to 114,079, accounting for 59 per cent of the industry workforce

Cybercrime

6 minutes
On average, a cybercrime report occurs every six minutes, remaining stable compared to 2023

up 17 per cent ($30,700)
Average self-reported cost of cybercrime per report for individuals

down 8 per cent
Average self-reported cost of cybercrime per report for businesses

47 million data breaches
Australia recorded 47 million data breaches in 2024, making it the 11th most affected country globally

4th most targeted nation globally
Australia emerged as one of the top five most targeted nations for cyber threats against critical infrastructure, now ranking 4th globally

Source:
Australian Cyber Network 2024 Annual Report

Open-Source Intelligence (OSINT) Publicly Available Information (PAI)
OSINT-PAI AI-as-a-Service (AIaaS) Actionable Analytics

AI/ML Automaton to Drive Actionable Cyber Intelligence

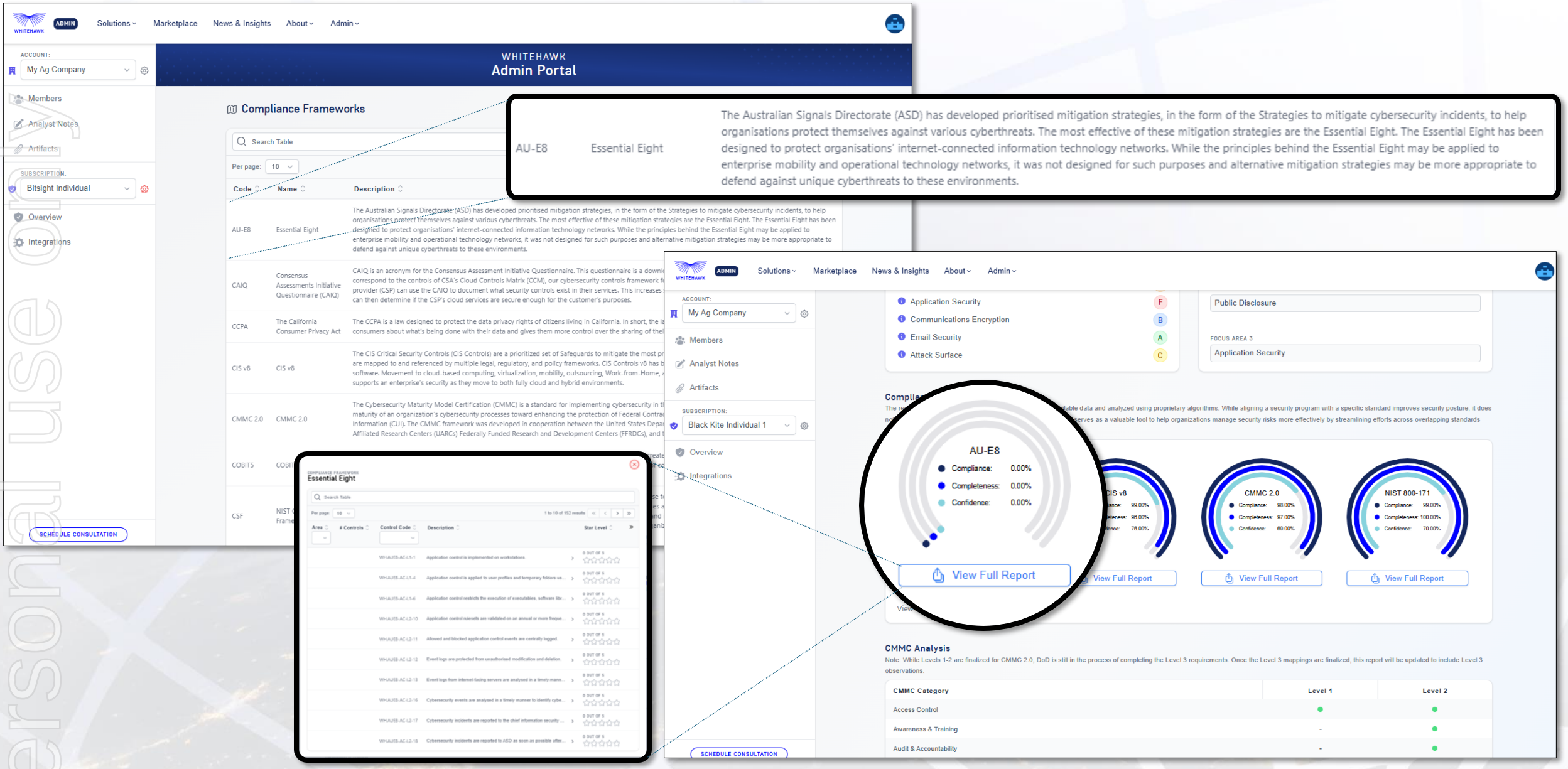
Fast-Track Big Data Collection, Correlation and Prioritization

Receive Actionable, Prioritized Analytics, Reporting, Strategies

Automate All Key Deliverables to Focus Workforce on Risk/Threat Mitigation

Basic AI/ML to Intermediate-Advanced-Predictive AI to Generative AI Across All Publicly Available Datasets

New Automated Path to the Australian Essential Eight



AU-E8 | Essential Eight | The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the Strategies to mitigate cybersecurity incidents, to help organisations protect themselves against various cyberthreats. The most effective of these mitigation strategies are the Essential Eight. The Essential Eight has been designed to protect organisations' internet-connected information technology networks. While the principles behind the Essential Eight may be applied to enterprise mobility and operational technology networks, it was not designed for such purposes and alternative mitigation strategies may be more appropriate to defend against unique cyberthreats to these environments.

2025 Strategy, Pipeline & Projections

Revenue Projections

2025 revenue projections now on track with current contracts, active, broad Commercial Pipeline (Healthcare & Academic Sectors) and Federal, State, Local Government RFPs

Customer Renewal

- 80% or greater
- Retaining Clients on average for 2-5years

New Sales Bookings

US$20M+ Pipeline to achieve growth benchmark $5.5M

- Cyber Risk Radar US$12.5M || Cyber Risk PaaS US$5M
- U.S. Government RFP Awards WHK US$4.2M

Employee Retention

- Maintain current excellent employee retention of 80%-90%
- Conversion of proven Interns to Full-Time
- Recruiting of new Cyber Interns

Existing Customer Upsell/Cross-sell

- Federal Government CISO US$750K
- Commercial CISOs US & AU $2.4M
- Research Universities US$4M || Consulting Groups US$1.2M

Product Roadmap Delivery

- Advancing AI-Roadmap with automation and scalability
- Delivering Integration with advanced cyber risk partners
- Automated CMMC Compliance Mapping into Action Plans

Cyber Risk Products Marketing & Branding

- C-SCRM Risk Radar, Cyber Risk Analyst PaaS, Cyber Risk Program
- PR, IR & Digital Marketing Campaigns in U.S. & Australia
- Cyber Innovation, Global Risk & CMMC Thought Leadership

Customer Needs Alignment

- Tailoring of platforms to meet evolving requirements
- Continuous advancement of platform features and new product lines

WHK Business Strategy Priorities 2025

Grow new Client Base Leveraging 2 new product lines:

1- AI-Based Critical Infrastructure Global & Regional Entity Illumination

2- Cyber Risk Analyst Platform as a Service

As Prime or in Partnership with Carahsoft & NUARI, continue to respond to U.S./Canada State & Local Opportunities like recent State of Ohio & City of Atlanta open RFP's

Advance LinkedIn & Dripify Campaigns developed with NYC Firm ESG, fully leveraging Hubspot - Focused on:

Phase 1 Healthcare

Phase 2 Universities

Continue to grow Consulting Firm Partnerships - 8 Degrees East, Zura Group, Hathaway Global Strategies – providing all product lines remotely

Retain, advance & grow current Cyber Risk Radar, Cyber Risk Program, Cyber Risk Analyst as a Platform contracts for recurring revenue & product advancement

Corporate Snapshot

ASX Ticker
WHK

Shares on issue
735.2 m

Last share price
A$0.015

Undiluted Market cap
A$11.0m

Net Cash
US$599k
as of 31 Mar 2025

Listing Date
24 Jan 2018

All figures are as of 19 May 2025 unless otherwise noted.

Top 5 Shareholders	% Shares
Lavya Pty Ltd	5.60%
Terry Roberts	5.10%
Mr Giuseppe Porcelli	4.76%
BNP Paribas Nominees Pty Ltd ACF CLEARSTREAM	2.64%
Mr Vince Zangari	2.29%
Top 5 Shareholders	20.39%
Top 20 Shareholders	35.2%
Directors & Associates	10.71%

U.S. Federal State/Local Pipeline

- **Won GSA SCRIPTS (Supply Chain Illumination Program, Tools & Services) 10 Year Contract Vehicle, $99M a year for 10 Years**
  16SEP24 Submission - Task Orders can start MAY25 to 4 Big Companies and 4 Small Businesses:
  - WHK selected as Cyber Sub to Knexus Research
  - Team includes Babel St, Dun & Bradstreet & WHK
  - Established engagement priorities to drive Client Task Orders to GSA Scripts Contract Vehicle

- **Responded to U.S. Defense Advanced Research Projects Agency (DARPA) Open BAA 10MAY25:** The Information Innovation Office (I2O) creates groundbreaking science and develops transformational capabilities in the informational and computational domains to surprise adversaries and maintain enduring advantages for national security.

- **Responding to: RFI SWFT Tools (Information for Software Fast Track for Tools) with Prime REI Systems 20MAY25**

- **Fall 2025 RFP: ASCOPE / PMESII Partner Capability Review with Prime LEIDOS**

- **When Administration reopens OSD CDAO Tradewinds Program: Submit w/ USF & NUARI https://www.tradewindai.com/**

- **WHK Cyber Resilience Moonshot: Engaging States of Florida (with Peraton), Maryland, Ohio and Dept of Defense OSD CIO/CISO**

U.S. Executive Order was signed "to consolidate federal procurement of goods and services within the GSA to remove waste and duplication and enable agencies to focus on their mission of delivering services to citizens. Within 90 days, the EO directs the GSA administrator to submit to the director of the Office of Management a comprehensive plan for consolidating the procurement of common goods and services across the government."

2025 Updated Contracts & Quotes (USD$)

Account Name		Date	Stage
Global Social Media Company TPRM Architecture & Risk Mitigation	$2.4M	12/24-12/26	Won
Georgetown University – Cyber Risk Program Renewal w/ CMMC 1 R&D Enclave CMMC 2 & Vendor Risk Baseline	$42K $45K $92K	04/25 04/25 05/25	3RD YR Renewed Under Review Under Review
Zura Group Proposal for Intel PEO	$780K	05/25	Awaiting Client PO
City of Atlanta Paid Cyber Risk Radar Pilot Follow-on City & Vendor Contracts for 3 YRS	$50K $92K	06/24 12/24	Won Won
NUARI SOCOM Information Ops R&D Platform - Entity Illumination RFP for Commercial Body of Knowledge: SOW 1 & 2	$66K $61K $330K	09/24 03/25 03/25	Won Won Pending
ASX 100 Company – Cyber Risk Program Cyber Threat, Fraud Prevention & Take Down Solutions/Services	$47K $500K	07/24 05/25	Won Under Board Review
Federal CISO Renewal Option Year 4 Working updated scoping for contract renewal 2025	$700K $700K	07/24 07/25	Renewed/Won In Process
University Cyber Risk Analyst Internship PaaS POV Annual Subscription & Additional Funding under review for 8 Universities	$25K $75K $1.3M	09/24 04/25 02/25	Won Under Review Working Gov't Funding
GSA SCRIPTS Contract Vehicle Task Orders	$1-2M	04/25 06/25	Won Sub-Contract Awaiting Task Orders
DARPA BAA	$350K	05/25	Submitted
Healthcare Proposals			Being Scoped

Australian & U.S. Cyber Internship & Research University Initiative

"Enhancing University and College Cybersecurity Programs with Practical Support for Courses, Degrees, Certificates, and Professional Certifications"

- Scale Impactful, Experiential Cyber Risk Analyst Internships Nationally:
  To grow cyber talent capacity and job opportunities
- Provide Foundational Cyber Risk Services to Small/Mid State, Local, Critical Infrastructure Entities To make our communities resilient
- Conduct Quality Research Across Cyber Risk/Threat Datasets & Analytics
  By providing trends by sub/sector, region, & size
- Measure implemented policies, best practices and solutions for impact on resiliency Proving what works

Exemplar Cyber Risk Analyst Internship Program

UNIVERSITY of SOUTH FLORIDA CLIENT Marketplace Client Portal

ACCOUNT: Orlando Health

Members
Analyst Notes
Artifacts

SUBSCRIPTION: Risk Rating

Overview
Integrations

UNIVERSITY OF SOUTH FLORIDA
Client Portal

‹ Back

CYBER RISK
Orlando Health

Scor

81
B
Expired on: 1/8/2025

Cyber Risk

The Cyber Risk measures a company's relative security effectiver
company falls into the 81-90 range, or B grade, meaning its relati
effectiveness is high, having a strong security performance and l

Vulnerability Heat Map

This heat map is the graphical distribution of vulnerabilities where the status and the severity of each finding are represented as the total number in each cell. Please note that 'Leaked Credentials' are represented as 1 (even if there are thousands) in order not to skew the chart.

	MEDIUM	HIGH	CRITICAL
WARNING	8	2	0
FAILED	61	46	20

Risk Vector Analysis

Security vectors and their outcomes are used to develop your company's Security Rating. Over 20 risk vectors are used in the Risk Rating determination. For simplicity, we have organized them into 7 groups.

Compromised Systems	A
Public Disclosure	F
System Patching	F
Application Security	C
Communications Encryption	C
Email Security	A
Attack Surface	B

Focus Areas

Based on the perceived risks derived from the risk rating and risk vector assessment, prioritize addressing these three focus areas to improve your cyber posture.

FOCUS AREA 1: System Patching

FOCUS AREA 2: Public Disclosure

FOCUS AREA 3: Application Security

FAIR Assessment

Factor Analysis of Information Risk (FAIR) is a quantitative risk analysis model that describes what risk is, how it works, and how to quantify it. This model specializes in financially derived results tailored for enterprise risk management, using Loss Event Frequency (LEF) and Loss Magnitude (LM) to calculate risk. LM answers the question "What will be the impact if there is a breach" while LEF calculates the likelihood of a breach. In other words, a formula of Annualized Risk Cost = LEF x LM.

Annual Loss Exposure

The forecasted annualized loss based on the given parameters below.

Minimum:	Average:	Maximum:
$7,179.00	$492,563.00	$3,104,643.00

Loss Event Frequency — 0.159

How many times over the next year is the loss event likely to occur?

Threat Event Frequency:	**55**
Contact Frequency:	245
Probability Of Action:	16.10%
Vulnerability:	**53.00%**
Threat Capability:	31.00%
Resistance Strength:	69.50%

Loss Magnitude — $3,104,643.00

How much loss is your organization likely to experience as a direct result of a loss event?

Primary Loss:	**$1,189,493.00**
Secondary Loss:	**$1,915,151.00**
Detection And Escalation:	$366,175.00
Notification:	$204,593.00
Post Data Breach Response:	$481,258.00
Lost Business:	$863,126.00

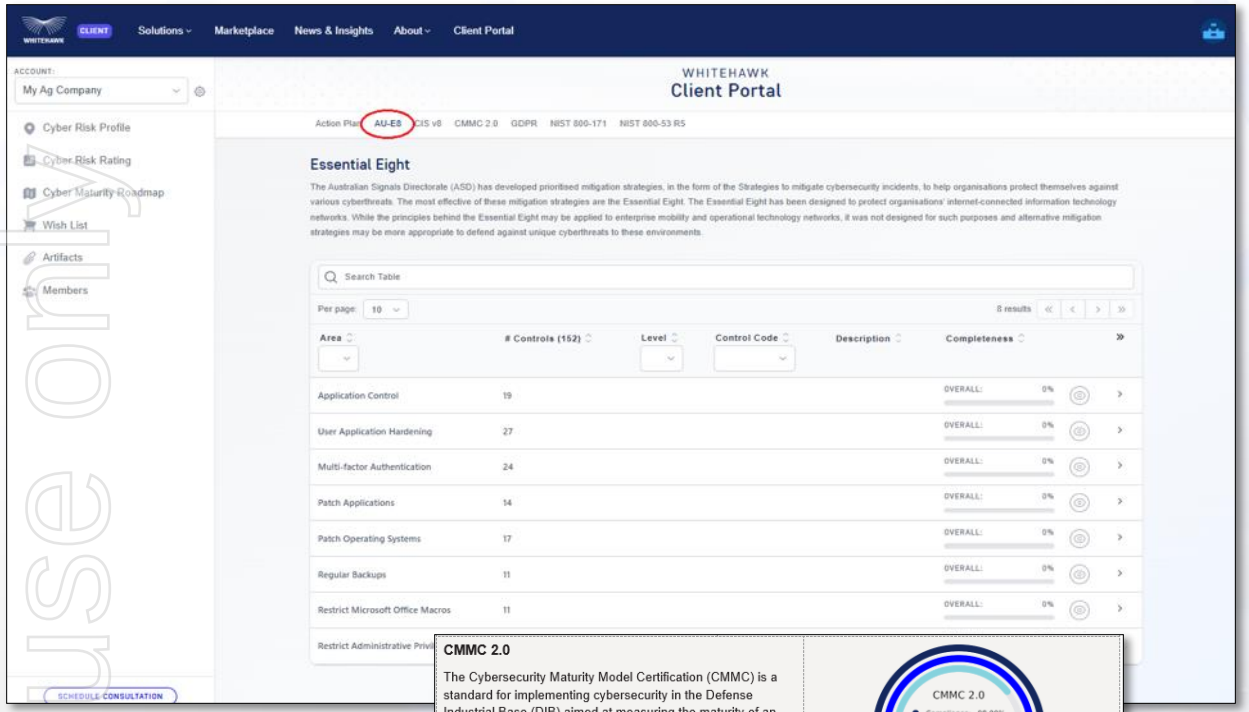
Compliance

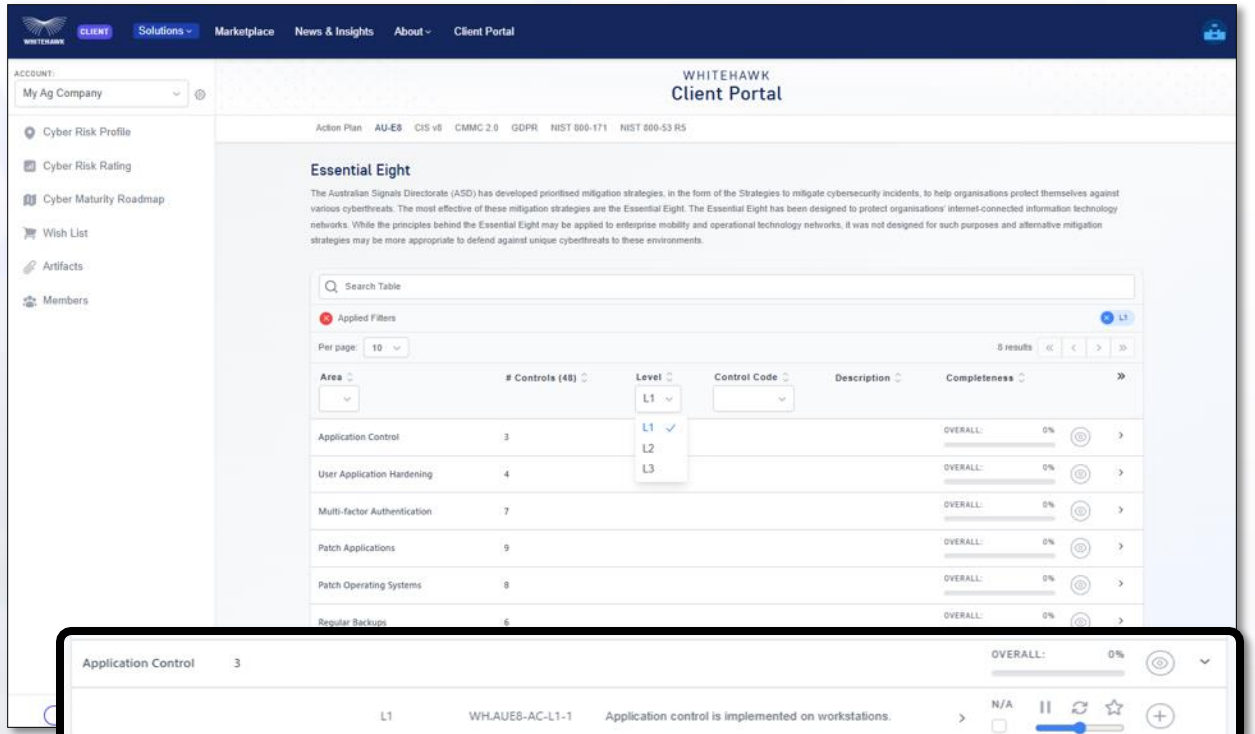
The compiled results are an estimation based on the publicly visible output correlated using proprietary algorithms. Companies that have aligned their security program to one of these standards should not assume that by so doing, they are in full compliance with the corresponding compliance standard. The crosswalk provides an informative tool for companies to use to help more comprehensively manage security risks in their environments by deduplicating the workload across different similar standards and best practices.

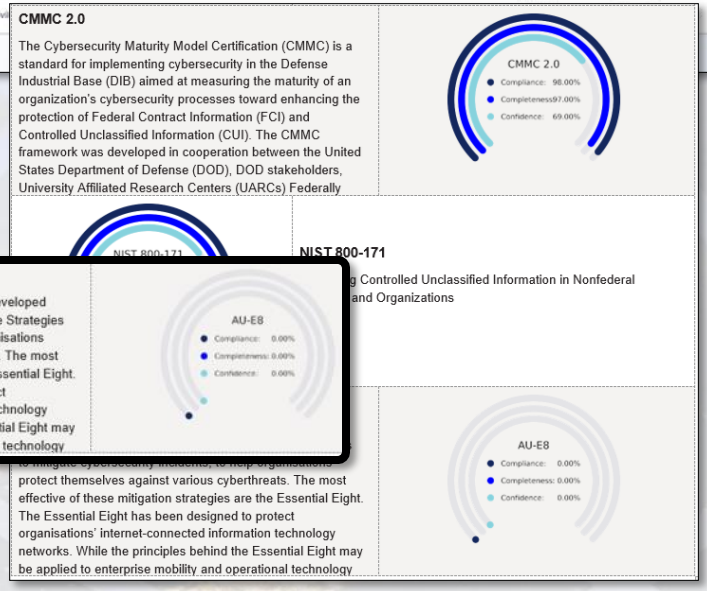
CAIQ	CCPA	COBIT19	CSF
Compliance: 100.00%	Compliance: 100.00%	Compliance: 100.00%	Compliance: 84.00%
Completeness: 8.00%	Completeness: 62.00%	Completeness: 10.00%	Completeness: 8.00%
Confidence: 55.00%	Confidence: 62.00%	Confidence: 56.00%	Confidence: 87.00%
View Full Report	View Full Report	View Full Report	View Full Report

CSF v2.0	GDPR	HIPAA	ISO27001
Compliance: 95.00%	Compliance: 100.00%	Compliance: 100.00%	Compliance: 100.00%
Completeness: 10.00%	Completeness: 67.00%	Completeness: 24.00%	Completeness: 9.00%
Confidence: 84.00%	Confidence: 69.00%	Confidence: 55.00%	Confidence: 57.00%
View Full Report	View Full Report	View Full Report	View Full Report

Continuous Essential Eight Risk to Resilience







Cyber Risk Analyst Internship Program Capability Overview

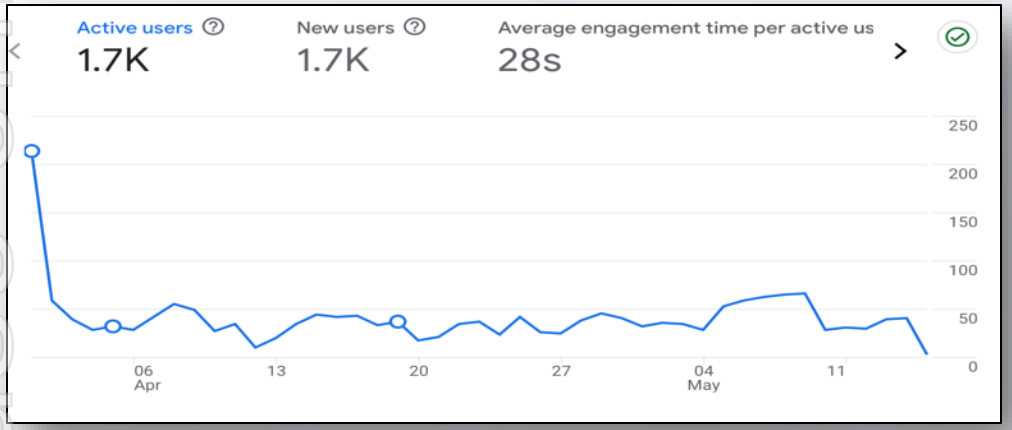
Over 30 Australian and over 300 U.S. Cyber Academic Institutions

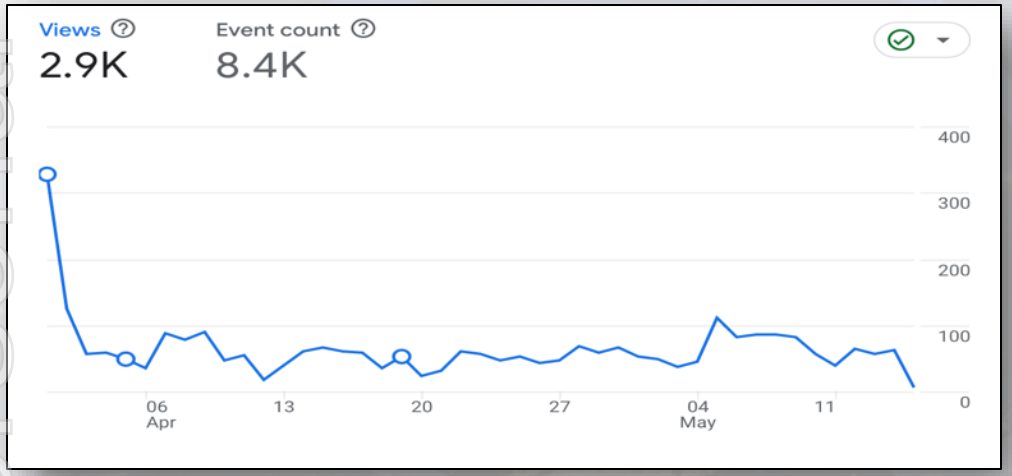
Annual Cyber Risk Analyst PaaS CAE University Subscription Includes:

- WHK Platform - White-labeled Client Portal
- 4 Training Sessions
- 5 Regions/Portfolio
- 2 Client Analyst Trainer Accounts
- 20 Active Analyst User Accounts
- 20 Entities (xyz.com): Continuous Cyber Risk Monitoring
- Annual Subscription $119k AUD or $75K USD per University
- Across the 30 AU Universities with Cyber Programs $3.5m Annually

Healthcare Online Campaign Round #2 Dripify Metrics – APR25

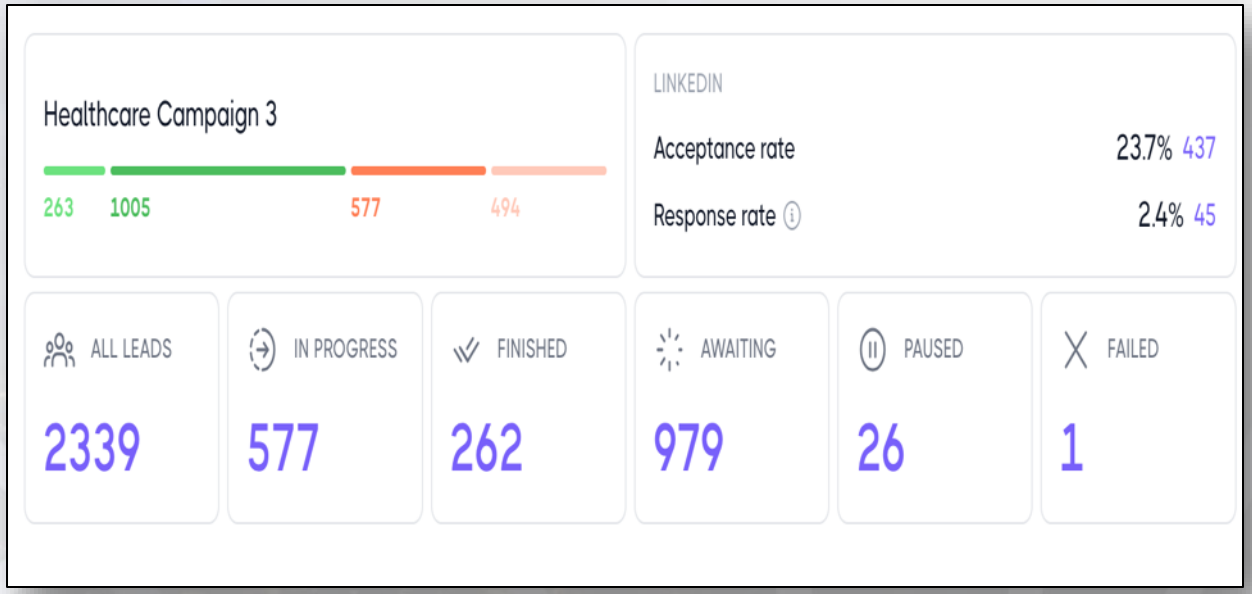
WHK Website Google Analytics





Dripify Leads Data – Healthcare Campaign

- All Leads: 2,339
- In Progress: 577
- Acceptance Rate: 23.% (437)
- Active Leads: 35
- Reply Rate/Direct Messages 2.4% (45)



Key Healthcare Leads: Premier Health & FHA

Independent Cyber Risk Program – A New Cyber Paradigm

Essential Annual Subscription Starting $17K a year per Healthcare Sector Entity

CYBER RISK IDENTIFICATION, PRIORITIZATION, VALIDATION & MITIGATION ROADMAP			
	Essential	Balanced	Premium
Virtual Consultation	✓	✓	✓
Continuous Cyber Risk Monitoring	✓	✓	✓
Quarterly Reviews and Deep Dives	✓	✓	✓
Continuous Business Risk Monitoring		✓	✓
Dark Net and Cyber Threat Intelligence Monitoring		Annually	Semi-Annually
SW-based Pen Testing - Risk & Compliance Validation		Annually	Semi-Annually
ADDITIONAL SERVICES			
Real Time Red Team			
Internal Network Risk & Threat Monitoring, Instrumentation, Integration & Quarterly Reporting			
Validated Risks & Mitigation Options Mapped to Resourcing Roadmap			
Additional Virtual SME Consults in Support of Executive Communication & Decision Making			

Annual Subscription Starting Prices:

- *Essential: $17,000*
- *Balanced: $115.500*
- *Premium: $131,000*

The Leadership Team

CHIEF EXECUTIVE OFFICER, PRESIDENT & FOUNDER

Terry Roberts

A global risk analytics, cyber intelligence and national security professional with over 20 years of Executive level experience across government, industry, and academia. Previously the Deputy Director of US Naval Intelligence, TASC VP for Intelligence and Cyber Engineering, and an Executive Director of Carnegie Mellon Software Engineering Institute (established the Emerging Tech Center now the AI Division) with an MSSI w/ AI concentration.

CHIEF OPERATING OFFICER & CHIEF PRODUCT OFFICER

Soo Kim

Previously the cybersecurity, technology strategy expert at Accenture Federal Services, Hewlett Packard Federal and VP at TASC. Experience in technical and business leadership, tactical execution, business operation, and solutions delivery. Bachelor's degree in mathematics from Virginia Tech, a Certified Enterprise Architect and Scrum Master and AI/ML Solution Architect.

CHIEF INFORMATION OFFICER

Mike Ferris

Technology executive with nearly 20 years of experience in IT and cybersecurity. Previous roles include Director of IT Operations & Security, Director of Advisory Services, and Senior Cyber Analyst & Program Manager. Led cybersecurity initiatives for both government and commercial entities, managing multi-year contracts focused on cyber and business intelligence, and regulatory compliance. Began his career as a Technical Controller in the US Marine Corps before transitioning to the commercial sector in 2010.

CHIEF TECHNOLOGY OFFICER

Michael Good

A Technical Program Manager with over 30 years of experience in cyber operations and technology development for military, government, and commercial cybersecurity solutions. Previous assignments include Raytheon, Vencore, L3 Communications and the US Census Bureau. Before entering private industry, Michael was a US Army Ops Research and Cyber Warfare officer at US Cyber Command, leading cyber operations planning for NSA's IA Directorate, with an MS in Computer Network Operations.

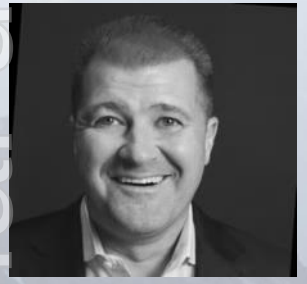
The Board

Phil George, Non-Executive Director

Phil George has experience as a CEO, managing director and operations manager with a strong background in finance, cybersecurity and technology. Philip has previously worked as a general manager, technical director, global IT manager, team lead and IT manager in other organisations. For the past 16 years, Phil has primarily serviced the finance, technology, mining industries and was recently the Operations Manager for Uber Australia. Phil is the Founder of NURV Consulting, which delivers custom cloud-based solutions to small and medium businesses and the Founder and CEO of Bamboo, a mobile micro-investment platform.

Melissa King, Non-Executive Director

Melissa King brings more than 20 years global experience as a senior executive, including her roles as Chief Executive Officer for the Australian Veterinary Association, FIBA Women's Basketball World Cup 2022 Organising Committee and Surf Life Saving Australia (SLSA) and executive roles with Sydney Opera House, Department of the Prime Minister and Cabinet APEC Australia 2007 Taskforce and the Governance Institute. A strategic, agile and innovative leader with extensive transformation, commercial and communications experience, Melissa has advised Boards and Government Agencies on strategy, governance and fundraising, and mentors emerging leaders.



Brian Hibbeln, Non-Executive Director

Brian Hibbeln is currently a venture partner at Sinewave Venture Capital LLC, a venture capital firm with the mission of accelerating new technologies across the public and commercial sector. He was the Director of the US Remote Sensing Center - National Capital Region (Washington D.C.) for almost a decade, being instrumental in supporting the DoD and Intelligence Community with technology demonstrations and operational support to combatant commanders around the world. Brian Hibbeln has advised Boards and Government Agencies on Cyber Technologies, Intelligence Activities, Mergers and Acquisitions and the deep understanding of Government needs or requirements. Mr. Hibbeln's extensive global networks and experience will open new channels for Whitehawk into the Australian, British and other markets globally.

Giuseppe Porcelli, Non-Executive Director

Giuseppe Porcelli is the Founder, Chairman & Group CEO of Lakeba Group Limited. A visionary entrepreneur, investor, and business leader with a proven track record in building and scaling innovative technology ventures, leading a global enterprise dedicated to developing and commercializing AI-driven solutions that optimize business operations, drive automation, and enhance digital transformation. Giuseppe is also the Chairman of Assetora (ASX: AOH), where he plays a pivotal role in guiding the company's growth and market strategy in fractional property investment. His expertise in corporate governance, M&A, and capital markets has been instrumental in driving strategic initiatives, including cross-border expansions and high-profile partnerships.