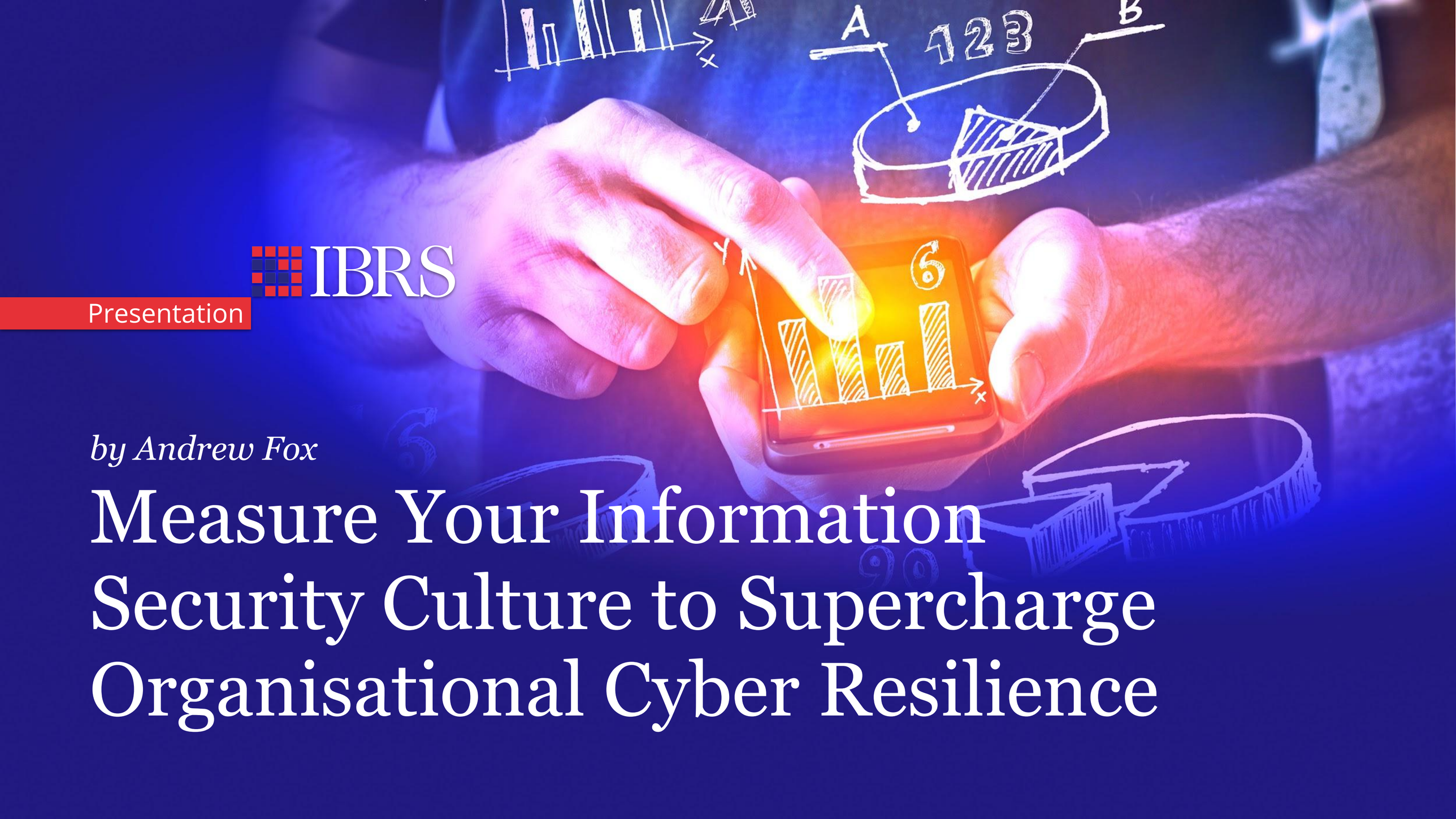



IBRS

Presentation

*by Andrew Fox*

# Measure Your Information Security Culture to Supercharge Organisational Cyber Resilience

# Introduction & Agenda

- Welcome
- The importance of measurement for building cyber resilience
- The human risk vector – a call to action
- Common frameworks from which we derive our cyber security awareness program (CSAP) controls
- The limitations of traditional CSAP controls
- Measuring employee behavior
- Measuring organisational culture
- Building a Resilient Human Firewall
- Summary

# “What You Cannot Measure, You Cannot Manage”

Metrics offer an objective way to evaluate your organisation's security posture.

- Build trust with key stakeholders by demonstrating the program's effectiveness.
- Providing evidence of the return on investment (ROI) of your cyber security programs assists in securing budget approvals.
- Demonstrate compliance and accountability by reporting on regulations and industry standards.
- Measure maturity and effectiveness to help identify areas for enhancement and prioritisation.
- Identify and mitigate you risk exposure, allowing for the implementation of strategies to mitigate potential threats.
- Metrics should also lead to quicker detection and response to incidents.
- Measures should be able to foster competition and accountability.

We should all have a set of metrics to measure the effectiveness of our cyber security programs.

# The Human Risk Vector

Cyber security is increasingly becoming a human challenge, and organisations are not adapting rapidly enough:

- Threat actors are increasingly targeting people as technical defenses mature.

  *Employees are involved in 68 per cent of all breaches globally.*

  *Verizon 2024 Data Breach Investigations Report*

- Generative AI has significantly contributed to the large increase in human vector attacks:

  *Since the launch of ChatGPT in November 2022, phishing emails have risen by a staggering 4151 per cent.*

  *SlashNext 2024 State of Phishing Report*

- The consequences of breaches are increasing:

  *43 per cent of organisations reported the loss of business-critical data or intellectual property, up from 34 per cent, indicating a rise in the severity of breaches.*

  *Fortinet State of Cyber Security Report 2024*

- Organisations are not keeping pace with these human vector attacks:

  *In 2023, 73 per cent of organisations faced Business Email Compromise attacks (BEC), yet only 29 per cent trained their users specifically to spot these threats.*

  *Proofpoint: 2023 State of the Phish Report*

# Common Cyber Security Frameworks

When developing our Cyber Security Awareness Program (CSAP), we draw from the cyber security framework adopted by our organisation.

- **NIST Cyber Security Framework (CSF):** Provides a flexible, risk-based approach to continuously assess, manage, and improve cyber security posture.
- **CIS Critical Security Controls (CIS18):** Offers a prioritized set of 18 controls designed to measure and improve an organisation's cyber security maturity by addressing the most common threats.
- **ISO 27001:** Enables organisations to measure their cyber security posture through a risk-based Information Security Management System (ISMS) and certification process.
- **Essential Eight:** Focuses on eight prescriptive controls to measure and mitigate common cyber threats, providing a baseline for cyber security effectiveness.
- **Information Security Manual (ISM):** A comprehensive framework that integrates risk management to measure and protect IT and operational systems against cyber threats.
- **Australian Energy Sector Cyber Security Framework (AESCSF):** An industry control framework that measures cyber security maturity and resilience against threats and regulatory requirements.

# Human-Centric Security Awareness Programs

- An effective Cyber Security Awareness Program (CSAP) should address behavior and culture to be effective.
  - An effective CSAP must go beyond implementing traditional cyber framework controls and seek to influence behavioral and cultural change.
  - A strong security culture is one in which the business shares a sense of mutual accountability.
  - The key to engaging the business lies in developing effective measurements of our: CSAP, employee behavior, and organisational culture.
- Human vector attacks are effective because they exploit human psychology, leverage trust, creating a sense of fear or urgency, and capitalise on curiosity or negligence.
- Human behavior directly amplifies or negates the effectiveness of technical security controls.

# Straw Poll

*Who believes they have an effective mechanism to evaluate their Cyber Security Awareness Program?*

IBRS

July 2025

# Example of Traditional CSAP Controls

**CIS Critical Security Controls® Version 8, Control 14:**

Security Awareness and Skills Training:

14.1 Establish and Maintain a Security Awareness Program.

14.2 Train Workforce Members to Recognise Social Engineering Attacks.

14.3 Train Workforce Members on Authentication Best Practices.

14.4 Train Workforce on Data Handling Best Practices.

14.5 Train Workforce Members on Causes of Unintentional Data Exposure.

14.6 Train Workforce Members on Recognising and Reporting Security Incidents.

14.7 Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates.

14.8 Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks.

14.9 Conduct Role-Specific Security Awareness and Skills Training.

# The Limitations of Traditional CSAP Controls

- Do not allow for the measurement of CSAP effectiveness:
  - Activity vs. outcome focus.
  - Lack of performance indicators.
  - No feedback loop for program improvement.
- Do not allow for the measurement of employee behavior and attitudes:
  - Knowledge vs. behavior gap.
  - There are no behavioral metrics.
  - Attitude remains intangible.
- Do not allow for the measurement of the organisation's security culture:
  - Culture is more than training.
  - No holistic cultural metrics.
  - Lagging indicators only.

CSAPs are limited by their focus on providing awareness which is about perception and cognition, instead of belief which involves acceptance and conviction.

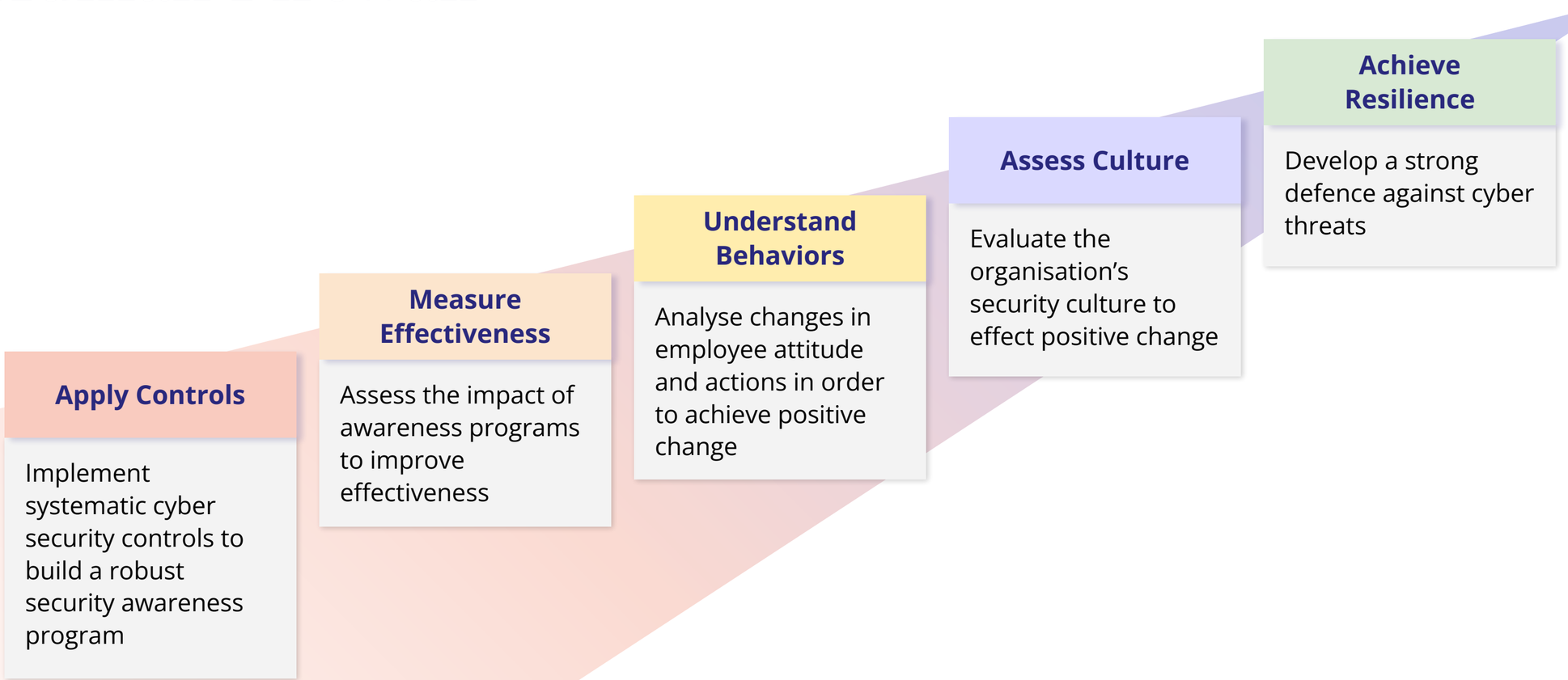
# Measuring Employee Behaviour

- **SANS Security Awareness Maturity Model:** a widely recognised model to assess the sophistication and effectiveness of a security awareness program, employee attitudes, and organisational culture.
- **Training/Phishing Simulation Platform Tools:** these platform not only offer comprehensive training modules, they provide phishing simulations and their reporting tools are increasingly providing metrics on human risk.
- **Behavioral Analytics Tools:** these platforms monitor user activity patterns, creating risk profiles through User and Entity Behavior Analytics (UEBA) to identify risky behaviors and policy adherence.
- **Interviews:** qualitative data gathering to understand unwritten norms and actual practices.
- **Gamification and Incentives:** measurement of participation and positive engagement in security-related activities through platforms that track points, badges, and leaderboards.
- **Implement a Human Risk Index (HRI):** an aggregated scoring systems that combines various behavioral indicators to create comprehensive risk profiles for employees/departments.

# Measuring Organisational Culture

- **SANS Security Awareness Maturity Model:** a widely recognised model to assess the sophistication and effectiveness of a security awareness program, employee attitudes and organisational culture.
- **Other Cyber Security Culture Assessment Tools:** Security Culture Maturity Models that provide structured assessments of organisational values, behaviors, and beliefs, generating security culture scores based on multiple dimensions.
- **Leadership Engagement Metrics:** tools tracking visible leadership championing of cyber security, including metrics on senior leaders discussing security in meetings, modeling secure behaviors, and supporting security initiatives.
- **Observation and Interviews:** qualitative data gathering to understand unwritten norms and actual practices.
- **Feedback and Communication Platforms:** internal systems and ambassador programs for fostering open communication about security concerns, tracking engagement in security-related discussions, and measuring the effectiveness of security communication channels.
- **Tabletop Exercises and Security Drills:** simulated activities that measure organisational response capabilities and reveal gaps in understanding, while fostering shared responsibility for cyber security.

# Building a Resilient Human Firewall



# Summary

- **The Human Element is Critical:** people are the primary target and the strongest defense. Ignoring human risk is no longer an option.
- **Measurement is the Key:** you can't improve what you don't measure. Effective measurement provides insights, demonstrates value, and drives continuous improvement.
- **Mature Your CSAP Program:** traditional CSAP controls are not sufficient. Leverage measurement tools and methodologies to guide your program's evolution from compliance-focused to being a strategic cultural driver.
- **Foster Competition:** create a culture of accountability, as teams strive to outperform one another in detecting and mitigating phishing attempts, ultimately reducing the risk of financial loss, downtime, and reputational harm caused by such attacks.
- **Foster Mutual Obligation:** cyber security is the responsibility of the entire business, not just the IT department.  Measure behaviours, attitudes, and culture to articulate this message.


Q & A
IBRS

*Submit an inquiry* or *schedule a whiteboard session*

IBRS

IBRS | ANALYSIS INSIGHT JUDGEMENT

IBRS is a boutique Australian ICT Advisory Company.

We help our clients mitigate risk and validate their strategic decisions by providing independent and pragmatic advice while taking the time to understand their specific business issues.

https://ibrs.com.au info@ibrs.com.au 02 4758 9111 PO Box 519, Hazelbrook NSW 2779, Australia