From Agentic Risk to Human Wins Report

Introduction

The corporate landscape in Australia and New Zealand (ANZ) has passed the point of theoretical AI experimentation; autonomous agents and machine-speed workflows are actively executing business operations.

However, as organisations scramble to capture efficiency gains, security postures are fracturing. KnowBe4's 'From Agentic Risk to Human Wins' Report highlights the critical blind spots, psychological vulnerabilities, and readiness gaps ANZ organisations are struggling with.

Section 1: The Shadow AI & Governance Deficit

While ANZ organisations introduce AI into their formal tech stacks, a significant unmanaged layer of "Shadow AI" is emerging across the region's workforces. Threat actors are keenly aware that security teams cannot protect assets they cannot see.

- 64% of surveyed organisations in ANZ deploy autonomous AI agents capable of taking actions on their own, yet 50% of leaders admit that AI usage within their perimeter is entirely unapproved or lacks formal corporate governance.
- Across ANZ, 59% of cybersecurity decision-makers report that the unsanctioned use of external software and rogue AI applications has directly degraded or actively compromised their security posture over the past 12 months.
- 59% of Australian workers admit to using unapproved tools outside policy and 57% say they intentionally use workarounds to bypass organisational security controls for productivity purposes.

Highlights

- **Discover the Governance Gap:** Uncover the extent of Shadow AI and why AI usage across organisations is often operating without formal corporate governance.
- **Assess the Agentic Shift:** Discover the percentage of organisations deploying autonomous AI agents capable of taking actions on their own, and the security consequences of that.
- **See the Psychological Battleground:** Learn how the threat vector has shifted to hyper-realistic, AI-engineered deepfakes and why most employees admit they could be successfully deceived.
- **Identify the Real Threat on Humans:** See the data on how cognitive overload and operational friction are forcing employees to cut corners, causing a significant percentage of security incidents.
- **Evaluate Your Readiness:** Understand the security maturity "Gold Standard" and find out whether security leaders feel resilient enough to survive emerging AI-driven threats.

Section 2: The Deepfake & Psychological Battleground

The threat vector has fundamentally shifted from traditional phishing to hyper-realistic, AI-engineered manipulation. Human cognitive defences are failing against machine-generated media.

- An overwhelming 85% of ANZ employees state that deepfake voice and video content is now so realistic that it is harder to know what to trust.
- 68% of the local workforce openly acknowledges that they could be successfully deceived by a sophisticated deepfake scam masquerading as an internal stakeholder or executive at work.
- Yet, 93% of ANZ organisations leaders remain confident that employees are able to identify impersonation messages via internal tools; 88% of ANZ organisation leaders are confident that employees can identify deepfake voice and video content.
- The threat landscape has transitioned from human speed to machine speed. ANZ organisations are structurally unprepared for automated, multi-stage attacks that target employees concurrently across email, SMS, and collaboration apps.

Section 3: Operational Friction & The "Gold Standard" Gap

The core threat is not simply advanced attacks; it is the compounding effect of human fatigue in high-pressure corporate environments colliding with low operational security maturity.

- 56% of ANZ employees confess that intense time constraints, cognitive overload, and everyday workplace distractions directly drive them to cut corners and make critical security errors, even when they are fully aware of safe protocols.
- One in four (24%) ANZ employees confess that they sometimes choose not to report a security mistake due to embarrassment. Yet, 93% of leaders in Australia believe that employees feel safe to report mistakes or suspicious activity without blame or embarrassment.
- Cybersecurity leaders in Australia & New Zealand highlight the scale of the behavioural gap, with almost all organisations (99%) reporting that human-related behaviours have impacted their cybersecurity over the past year.

Conclusion

The workforce in ANZ has changed. Employees and AI agents now operate as a single, interconnected layer of defence. That changes what good security looks like. Organisations that align awareness, behaviour and culture around a clear picture of their risk do more than simply managing exposure. They create hard targets. The threats won't disappear but they'll run into better prepared organisations.

KnowBe4, Inc. | Part Level 1, 95 Coventry Street, Southbank, VIC, 3006 Australia
+61 (1800) 577568 | www.KnowBe4.com | Sales@KnowBe4.com