# From Agentic Risk to Human Wins Report

## Introduction

The corporate landscape in the United Arab Emirates (UAE) and Saudi Arabia (KSA) 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 the UAE & KSA organisations are struggling with.

## Section 1: The Shadow AI & Governance Deficit

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

- 76 of surveyed organisations in the UAE & KSA deploy autonomous AI agents capable of taking actions on their own, yet 24% of leaders admit that AI usage within their perimeter is entirely unapproved or lacks formal corporate governance.
- Across the UAE & KSA, 52% 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.
- 41% of local workers admit that if official corporate AI tools are restricted or too slow, they will actively source their own unapproved agentic AI tools to bypass administrative blocks.

## 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 88% of employees in the UAE & KSA state that deepfake voice and video content is now so realistic that it is harder to know what to trust.
- 52% 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.

## Section 3: Operational Friction & The Improvement 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.

- 44% of the UAE & KSA 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.
- Cybersecurity leaders in the UAE & KSA confirm the severity of this behavioural gap, noting that up to 54% of all security incidents impacting their perimeters this year were triggered by everyday operational slips rather than exploit kits.
- Although 76% of security leaders feel "very well prepared" to handle unexpected or emerging AI-driven threats over the next year, 84% of them confirmed that improvements are still needed to ensure AI tools and agents operate within organization's security policies and approved risk limits.

## Conclusion

The workforce in the UAE & KSA 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. | Arjaan Office Tower, Offices 901-902, Dubai Media City, Dubai, UAE
www.KnowBe4.com | Sales@KnowBe4.com