knowbe4

UNITED KINGDOM

From Agentic Risk to Human Wins Report

Introduction

The corporate landscape in the UK 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 British organisations are struggling with.

Section 1: The Shadow AI & Governance Deficit

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

- 48% of surveyed organisations in the UK deploy autonomous AI agents capable of taking actions on their own, yet 51% of leaders admit that AI usage within their perimeter is entirely unapproved or lacks formal corporate governance.
- Across the UK, 58% 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.
- 21% of UK employees say they don't always use official corporate AI tools provided by their organisation, increasing the risk of unknown AI tools on corporate networks and posing a significant security risk.

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 British employees state that deepfake voice and video content is now so realistic that it is harder to know what to trust.
- 73% 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.
- The threat landscape has transitioned from human speed to machine speed. British 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.

- 47% of UK 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 UK confirm the severity of this behavioural gap, noting that up to 41% of all security incidents impacting their perimeters this year were triggered by everyday operational slips rather than exploit kits.
- Despite widespread awareness, a mere 20% of UK organisations have achieved a "gold standard" maturity model—defined as a fully synchronised culture capable of managing human and agentic risks in tandem.
- Furthermore, only 84% of security leaders in the UK feel resilient enough to survive unexpected or emerging AI-driven threat vectors over the next calendar year.

Conclusion

The workforce in the UK 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. | 1 Leeds City Office Park, Meadow Lane, Leeds LS11 5BD
01347 487512 | www.KnowBe4.com | Sales@KnowBe4.com

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.