CYBERCRIME NEWS

ISSUE 21 • JUNE 2026

AGENTIC AI

THINK BEFORE YOU AUTOMATE

AGENTIC ARTIFICIAL INTELLIGENCE (AI) TOOLS ARE MAKING THEIR WAY INTO ORGANISATIONS, OFFERING NEW OPPORTUNITIES FOR AUTOMATION. AGENTIC AI CAN BE BENEFICIAL, SUCH AS IN CYBER SECURITY DEFENCES, BUT IT CAN ALSO INTRODUCE NEW RISKS, IF NOT USED CAREFULLY.

WHAT IS AGENTIC AI?

Agentic AI can act without continuous human interaction to complete specific tasks. Agentic systems can access data sources, remember context, make decisions, use tools, and take actions in pursuit of a goal. However, they are not without risk. For example, agentic AI could be utilised by a retail company by using an AI system that not only responds to customer issues but also carries out actions—such as issuing refunds or arranging replacements—without human intervention.

WHAT ARE THE RISKS?

The extra autonomy and complexity of Agentic AI systems can pose significant risks to organisations.

Their behaviour can be hard to predict, test, and govern. Other risks include:

- **Non-restricted access** – Allowing Agentic AI access to external systems, data, and tools, can pose security risks if not managed effectively.
- **Unpredictability** - Because Agentic AI makes its own decisions, it may take unexpected actions that weren't explicitly planned or anticipated for.
- **Harder to spot problems** – Again, because of its independence, mistakes and errors may occur subtly, particularly when actions occur faster than humans can review them.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

ADOPTING AGENTIC AI CAREFULLY

If an agent has excessive privileges or is poorly designed, a single mistake can rapidly escalate into a major issue. It's therefore essential to pause and think carefully before deployment. You should:

- Evaluate what could go wrong and how failures or misuse could affect operations
- Consider whether AI is necessary, or if the process could be simplified in a lower-risk way
- Introduce Agentic AI gradually – start with tightly controlled pilots on clearly defined tasks and expand only once the system has proven reliable
- Insist on human accountability – It must be clear who owns, approved its access, monitors its behaviour, and reviews its incidents. These responsibilities should be defined before the agent is connected to real systems and data. Crucially, responsible individuals must be empowered to intervene if necessary.

FOR FURTHER INFORMATION

ETSI EN 304 223: Securing Artificial Intelligence (pdf)

This document outlines baseline cyber security requirements for AI systems, including agentic systems.

CONCLUSION

Agentic AI is likely to offer significant benefits in many scenarios: Start small, apply existing cyber hygiene and governance from the start and plan for failure, including who is responsible and the measures that will be taken to respond.

DORSET POLICE

Dorset Police

Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

E cybercrimeprevention@dorset.pnn.police.uk
www.dorset.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

Office of the Dorset Police & Crime Commissioner

Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

T 01202 229084
E pcc@dorset.pnn.police.uk
www.dorset.pcc.police.uk