Microsoft Security

# UK manufacturers recognise the potential of AI in cybersecurity

Over the past decade, manufacturing companies have undergone a significant digital transformation, adapting to external pressures and seizing new opportunities, leading to fundamental business model changes towards recurring revenue models. Looking ahead, manufacturers aim to invest in AI and IoT but will need to pay close attention to cybersecurity as cybercriminals become more sophisticated.

Given the vitality of a secure manufacturing industry to the UK economy, Microsoft collaborated with a team of researchers from Goldsmiths University to survey manufacturing businesses to find current levels of cyber resilience.

## Key findings

### AI-enabled cyberattacks pose a threat to UK manufacturing

In recent years, UK manufacturers have become accustomed to ongoing political tensions disrupting operations and supply chains.

**56%**

**of UK manufacturing decision makers surveyed** are concerned about ongoing political tensions, currently disrupting operations and supply chains, also presenting an increased risk of cyberattacks to their business.

**76%**

of those surveyed agree that the UK needs stronger cybersecurity defences if it wants to become an AI superpower.

**20%**

of manufacturing organisations surveyed currently use AI to detect cybersecurity vulnerabilities, although most manufacturing organisations are not prepared to encounter AI-enabled cyberattacks.

### AI-enabled defences can boost resilience and reduce costs

AI can be part of the solution to an increasingly sophisticated breed of cyber threats. By deploying AI-enabled defences, manufacturing organisations can become twice as resilient to cyberattacks and suffer 20% fewer costs when breached. The widespread adoption of AI for cybersecurity could save the national economy £52 billion every year.

### Road to resilience

The researchers used the new cybersecurity model to evaluate the effectiveness with which UK organisations are currently deploying AI-enabled cybersecurity solutions before grouping them into three categories: resilient, vulnerable, and high risk.

### How prepared are businesses for cyber threats?

13% Resilient

48% Vulnerable

39% At High risk

Making more organisations resilient and able to withstand AI-enabled cyber threats is essential for the country to achieve a prosperous future as a global centre for AI innovation and talent. The proportion of businesses that currently sit outside of the 'resilient' category shows there's progress that needs to be made. For manufacturers to make this happen, it requires a commitment to widespread adoption of AI-enabled technologies, seeking solutions that deliver fast ROI, training workers to be proficient in the technology, and sharing knowledge.

### Building resilience for the future

Many manufacturers have already rebalanced their supply chains with a focus on resilience to reduce future disruption and minimise supply. Now is the time to take a similar approach with cybersecurity to become more resilient and better protected against future threats.

**Access the full report:**

**Mission Critical: Unlocking the UK AI Opportunity Through Cybersecurity**