Microsoft Security

The Healthcare Sector Recognises AI's Impact on Cybersecurity

Amid exciting advancements, AI is unlocking new ways for the UK healthcare sector to improve patient outcomes. For example, AI-driven image analysis is enhancing early breast cancer detection, safeguarded by robust security features. However, the sector must safeguard patient data against cybersecurity threats. This article explores findings from a Microsoft UK study on mitigating these risks.

Key findings

1. Climate of concern

81% of those surveyed are concerned about malware attacks, **70%** about data breaches and **63%** about phishing and ransomware

While **80%** of healthcare organisations surveyed take preventative action against cyber threats,

17% of employees remain uncertain about their employer's protocols.

64% of healthcare organisations surveyed provide training on cyber threats and risks,

but **23%** do not offer such training, leaving a significant portion of the workforce vulnerable.

of healthcare organisations surveyed have been affected by a cyber attack in the last 12 months.

2. AI potential

A majority of the healthcare leaders surveyed (85%) acknowledge the importance of cybersecurity, seeing AI as a critical tool to bolster defences.

AI-enabled cybersecurity measures can significantly reduce the risk of cyber attacks, making organisations twice as resilient and reducing costs by 20% when breaches occur.

Widespread adoption of AI in cybersecurity could save the national economy billions annually, reflecting the substantial financial benefits of enhanced security measures.

The AI opportunity and the road to resilience

The healthcare sector faces unique challenges that make AI adoption both critical and transformative.

- Using advanced technologies is necessary to maintain operational efficiency and patient safety due to regulatory environments, financial strain, clinician burnout and workforce shortages.
- Enhancing the resilience of healthcare organisations to AI-enabled cyber threats is essential for ensuring patient safety and maintaining trust in healthcare services, making it an urgent priority.

Recommendations for resilience

To bolster healthcare organisations' cyber resilience, leaders should commit to the following actions:

1. Incorporate AI technologies into the organisation's cybersecurity strategy
2. Concentrate spending on effective buy-and-build configurations and off-the-shelf solutions that deliver a strong return on investment
3. Cultivate and develop the talent needed to address current and future cyber challenges
4. Promote the sharing of knowledge and open sourcing of research breakthroughs
5. Work with governments and policymakers to implement the National Cyber Security Centre's guidelines for secure AI system development

Onwards and upwards

Achieving widespread resilience in the healthcare sector relies on the actions of individual organisations. Practical steps include:

Assess and understand the unique threat landscape for the organisation on local, regional and national levels

Embrace AI-enabled cybersecurity solutions to mitigate attack risks

Allocate budget for technological upgrades and cybersecurity costs, ensuring a comprehensive recovery plan is in place

Identify and address the talent needs for an AI-enabled workforce

Move beyond understanding AI to actively innovating with it

Access the full report:

Mission Critical: Unlocking the UK AI Opportunity Through Cybersecurity