UK cyber agency warns of AI-powered ransomware against critical infrastructure by 2028



The UK's NCSC says AI-powered malware is highly likely to feature in a ransomware attack on critical national infrastructure by 2028. It stresses that long-tolerated weaknesses, not new attack methods, drive the risk.

- The NCSC's State of the Cyber Nation report says AI-powered malware is highly likely to be used in a ransomware attack on UK critical infrastructure by 2028.
- Within two years, hostile use of AI is highly likely to raise the scale and efficiency of ransomware, social engineering and vulnerability exploitation.
- The NCSC's CEO says the risk comes from tolerated vulnerabilities being found and exploited at scale, not from AI inventing new attacks.
- Recommended choices: invest adequately in technology, avoid unnecessary internet exposure, and

treat Cyber Essentials as a starting point.

- The UK government has announced funding for a national Cyber Shield, a vulnerability exposure centre and an AI security centre of excellence.

The UK's National Cyber Security Centre (NCSC), part of GCHQ, has published its State of the Cyber Nation report. It warns that critical national infrastructure should be prepared for a ransomware attack involving AI-powered malware by 2028, and that within two years hostile actors' use of AI is highly likely to increase the scale and efficiency of ransomware, social engineering and vulnerability exploitation.

What the NCSC is saying

The NCSC's CEO, Dr Richard Horne, frames the issue as one of foundations rather than novelty. In his words, an unprecedented rise in incidents is a real prospect, but not because AI has invented new ways to attack. Instead, vulnerabilities tolerated for too long can now be discovered and exploited at a scale once unimaginable. He describes an era of "tech on the cheap" that must end.

The report asks organisations to use tools, standards and frameworks that already exist and are evidenced to protect against both conventional and AI-powered attacks. Specific choices include investing adequately in technology, not leaving technology needlessly connected to the internet, and treating Cyber Essentials as the starting point, with resilience built up according to size, complexity and risk.

Government response

The UK is pursuing the Cyber Security and Resilience Bill and a forthcoming National Cyber Action Plan. Announced funding includes £60 million for the first phase of a national Cyber Shield, £70 million for a National Exposure and Real-Time Vulnerability Centre, and an AI Cyber Security Centre of Excellence in Manchester run by the NCSC.

Relevance for Saudi institutions

The report is a UK assessment, but its message applies to any regulated operator: AI shortens the time between a weakness existing and being exploited. Institutions can use it as a prompt to review basic hygiene, exposure and investment against their existing NCA and SAMA obligations.

What to do now

1. Review internet-facing assets and remove or restrict any system that does not need to be exposed.
2. Check that patching and vulnerability management cover legacy systems, with clear ownership and timelines.
3. Confirm that baseline controls under NCA ECC and, where applicable, SAMA CSF are fully implemented before adding new ones.

4. Update ransomware response and recovery plans, and test them against a scenario with faster, larger-scale exploitation.
5. Brief executives and the board on the underinvestment risk in technology and security, using your own risk assessment.