UK Enters 2026 Amid Rising Cyber Pressure Driven by Regional Geopolitical Tensions, New Security Bill Underscores Urgency

Monday 19 January, 2026

Related Sectors:

Business & Finance ::

Related Keywords:

Artificial Intelligence :: IT Security :: Cybersecurity ::

Scan Me:

Security expert Keith Poyser notes: “The disparity between increasingly aggressive tactics used by cybercriminals and state-sponsored threat actors, and organisations’ defensive capabilities continues to grow. Addressing this requires a move towards proactive, offensive security.”

London, 19 January 2026 – Security expert Keith Poyser, Vice President for EMEA at Horizon3.ai, warns that the gap between the aggressiveness of cybercriminals and state actors, and companies’ ability to defend themselves is widening, calling for a decisive shift towards offensive security practices. Poyser explained: “Cybercriminals and state-backed threat actors are acting faster, more aggressively, and with far greater innovation—especially through the use of artificial intelligence—while too many businesses continue to rely on traditional defensive methods. This widening gap must be closed urgently.”

These challenges arrive at a pivotal moment, as the UK prepares to introduce its new Cyber Security and Resilience (Network and Information Systems) Bill. Introduced to Parliament in late 2025 and expected to progress through 2026, the legislation is designed to significantly strengthen the UK’s cybersecurity framework. It will broaden the range of organisations that must meet higher cyber standards – including managed service providers, data centres, and critical suppliers – tighten cyber-incident reporting requirements so that regulators are notified more quickly during an attack, and give regulators stronger enforcement powers to drive compliance across essential and digital service sectors.

Poyser added: “Organisations must take proactive steps now—before regulations tighten further—to understand their real exposure and strengthen resilience. Offensive security approaches, such as continuous, autonomous pentesting, provide the evidence needed to stay ahead of attackers rather than reacting after the damage is done.”

A Simple Analogy Shows What’s Wrong With Traditional Security Models

The growing gap in cyber readiness is driven largely by companies’ continued reliance on passive defence technologies—firewalls, antivirus tools, intrusion detection systems—without ever validating whether these controls would actually function under real attack conditions. Simply installing security tools is no longer enough; organisations must prove that those tools work when it matters.

“This approach is like installing an elaborate alarm system in your home without checking whether it actually sounds during a break-in,” said cybersecurity specialist Keith Poyser. “In 2026, it is well past time for a fundamental shift towards offensive security methods. To keep the analogy going: you need to hire burglars to see whether they can bypass the alarm system. Any weaknesses they uncover must be fixed quickly—and then you must test again to ensure new weaknesses haven’t emerged. If you want real criminals to fail, this process can never stop.”

“In cybersecurity, that real-world test is called a penetration test—or ‘pentest’,” he explained. “But instead of hiring a burglar once in a while, companies now have access to autonomous pentesting platforms—effectively a robotic army of benign intruders that test your systems continuously.”

Understanding Risk Through the Eyes of the Attacker

These platforms, he adds, behave much like modern cybercrime groups. They share intelligence, learn from each other’s successes, and exploit the same weaknesses across multiple environments. “A flaw that allows a break-in at one organisation is almost certainly present in another using the same technology stack. This is exactly how today’s cybercriminal gangs operate, adjusting and improving their techniques as they move from target to target.”

By adopting autonomous offensive security methods, businesses can finally match the speed and ingenuity of attackers—moving from assumptions to evidence, and from reactive defence to continuous resilience.

“It is increasingly unrealistic for corporate security teams to maintain an accurate understanding of their true risk exposure using only traditional, passive methods,” said Keith Poyser. “Threat actors do not wait

for annual audits or one-off checks. Unless organisations test their systems in a way that reflects how real attackers operate, they will continue to be caught off-guard."

Replacing Guesswork With Evidence in Cyber Risk Decisions

Modern attackers think in terms of opportunity — moving from an initial access point through a chain of weaknesses to reach valuable assets. To address this, Horizon3.ai extends its offensive security platform with a capability called Threat Informed Perspectives. This approach gives security teams a view of their environment through the attacker's lens, showing not just individual weaknesses but how an adversary could realistically exploit them, how far they could move, and how quickly they might reach critical systems.

What sets this capability apart is its focus on actionable, measurable security improvement rather than raw data. Realistic attack scenarios from defined starting points — such as compromised credentials or misconfigured cloud services — allow organisations to identify where defensive controls fail and prioritise the steps that will have the greatest impact on reducing real risk. Over time, teams can track whether their exposure is genuinely shrinking and demonstrate progress in terms that executives, auditors and regulators can understand.

Poyser added: "Organisations need evidence, not assumptions. By aligning security validation with how attackers think and move, you get a much clearer picture of where your defences are working — and where they are not. That clarity is essential if businesses are to build meaningful resilience against evolving threats."

About Horizon3.ai.

Horizon3.ai's NodeZero® platform is trusted by over one-third of the Fortune 10 companies, the world's largest banks, top global pharmaceutical and semiconductor manufacturers, critical infrastructure operators around the globe, and the US Defense Industrial Base to proactively find, fix, and verify exploitable vulnerabilities to continuously fortify cyber defenses and improve cyber resilience. The fastest-growing cybersecurity company in America (Inc. 5000, Deloitte Fast 500), Horizon3.ai was founded by a mix of US Special Operations veterans and industry experts and is headquartered in San Francisco.

Follow Horizon3.ai on LinkedIn and X.

Trademark notice: NodeZero is a trademark of Horizon3.ai

Further information: Press contact: Stephen Gates - press@horizon3.ai, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Web: www.euromarcom.de, Email: team@euromarcom.com

Company Contact:

_

news aktuell

E. desk@newsaktuell.de
W. https://www.newsaktuell.de/

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.newsaktuell.pressat.co.uk