HORIZON3.ai
~~TRUST BUT~~ VERIFY

Horizon3.AI Europe GmbH

08.12.2025 – 12:41 Uhr

Offensive Security Becomes Business-Critical as UK Faces Major Cyber Incidents

London (ots) -

• Surge in major cyberattacks across the UK in 2025 of 50%

• Significant spend on Defensive Cyber tooling continues, as does the number of headline breaches.

• Organisations urged to treat cybersecurity as a board-level priority

• Horizon3.ai warns that organisations must adopt an offensive security approach – continuous, autonomous pentesting to stay ahead of AI-based attacks.

The scale, frequency, and sophistication of cyberattacks in the UK have escalated sharply throughout 2025, causing widespread operational disruption and mounting economic damage. Recent data and high-impact incidents show that organisations can no longer rely on periodic audits or reactive security measures. As a result, organisations are being challenged to rethink their security strategy and embrace an offensive mindset.

Major UK Attacks Rise By More Than 50%

The National Cyber Security Centre's (NCSC) Annual Review 2025, covering the period from September 2024 to August 2025, underscores the severity of the situation. During this time, the NCSC handled 204 nationally significant cyber incidents—an increase of more than 50% compared to the previous year. The review also reported four high impact attacks every week, each capable of disrupting essential services across the country and causing widespread operational and economic disruption. In worst case scenarios, such attacks could compromise not only business operations but critical national infrastructure too. The government is now urging organisations to take stronger action to protect the UK economy and make cyber resilience a board-level responsibility.

The economic stakes are equally stark. The recent cyberattack against Jaguar Land Rover—which is thought to be the largest cyber incident in UK history—has been estimated to cost the UK economy £1.9 billion. This led to Jaguar Land Rover having to shut down systems across their factories and offices, with knock-on effects extending to as many as 5,000 organisations in its supply chain.

Richard Horne, Chief Executive of the NCSC, issued a clear warning: "Cyber security is now a matter of business survival and national resilience. The best way to defend against these attacks is for organisations to make themselves as hard a target as possible."

Offensive Security: Thinking Faster Than the Attacker

Keith Poyser, Vice President for EMEA at Horizon3.ai, explains that organisations can only become "harder targets" by adopting an offensive, attacker-like mindset: "Organisations must think faster than potential attackers. All attack surface, ongoing penetration testing is the only reliable way to determine whether hackers can break in and whether an organisation's security controls are genuinely effective. Validate your defences in the context of your environment, don't guess or rely on noisy low relevance vulnerability lists alone"

Although penetration testing has existed for decades, it has traditionally been conducted only annually or quarterly, and purely by humans, which is no longer adequate given the speed at which attackers evolve. We have already seen AI tools misused to rewrite attacks on the fly adapting to defences or detection technologies.

Continuous, autonomous pentesting via platforms such as Horizon3.ai's NodeZero® Offensive Security Platform allow organisations to validate their security posture as frequently as needed—even daily—without the cost, delays, or limitations of manual-only tests. With them, businesses can emulate attacker techniques in live environments and integrate them seamlessly with agile and DevOps workflows, aligning security testing with how software is actually built and deployed today.

Too Many Organisations Rely on Defence

Horizon3.ai's own Cybersecurity Report UK 2024/25 which collected responses from managers with IT level responsibility in 150 UK organisations confirms that many organisations are not taking the right approach to face today's rapidly evolving threat landscape. When asked whether they take a purely defensive stance against cyber threats, or if they conduct offensive exercises to identify risks and vulnerabilities, results showed that 34% reported using only defensive measures, 21% focus on defence but occasionally conduct offensive exercises, and only 12% conduct offensive exercises internally. A further 15% were unsure how to approach this, while 18% said they outsource offensive exercises entirely.

Another question asked which technology, solution or practice they believed would significantly improve their security. 12% said they would want more budget funds, while 37% said they want to know exactly where they are vulnerable so they can proactively address weaknesses—a clear indication of the need for autonomous penetration testing. 26% responded that they would need to convince the leadership that cybersecurity must be a top priority.

Cybersecurity Must Become a Board-Level Responsibility

Government bodies, industry regulators, and customers are increasingly urging CEOs, boards, and senior leaders to take explicit, personal ownership of cyber risk. This shift reflects a broader recognition that cybersecurity is now a core component of organisational stability, operational continuity, and economic resilience.

Penetration testing plays a pivotal role in meeting these heightened expectations and has become a cornerstone of both operational and economic resilience. By continuously validating defences, organisations can reduce their Mean Time to Remediate (MTTR), lower the cost of fixing weaknesses, and significantly strengthen their overall security posture. Regular testing also supports risk-based vulnerability management, enhances audit readiness, and creates a verifiable record of due diligence—ultimately easing the burden of compliance.

Due Care and Due Diligence as Foundations of Cyber Risk Management

In cybersecurity, two fundamental principles form the backbone of effective risk management: due care and due diligence (Paired with a duty to know). Due care refers to the proactive steps an organisation takes to protect its systems, data, and users—such as enforcing security policies, fixing weaknesses, and carrying out regular risk assessments.

Due diligence, on the other hand, is the ongoing validation of whether those protective measures are actually working. It involves activities such as penetration testing, reviewing third-party risks, and verifying alignment with industry standards. Where due care is about implementing safeguards, due diligence is about proving they stand up in real-world conditions.

Keith Poyser added: "Together, they ensure that organisations are not only putting security controls in place but also continuously confirming their effectiveness. Continuous pentesting is central to this process, providing the evidence organisations need to demonstrate their cyber resilience."

About Horizon3.ai

Horizon3.ai empowers organisations to continuously verify their security posture with NodeZero®, the industry's leading autonomous pentesting platform. Built to think and act like an attacker — but operate safely in production — NodeZero identifies exploitable weaknesses, prioritises fixes based on real-world impact and verifies remediation at scale. Customers across manufacturing, healthcare, finance and national security rely on NodeZero to reduce risk and accelerate security outcomes.

Follow Horizon3.ai on LinkedIn and X.

Contact:

Further information: Horizon3.AI Europe GmbH, Prielmayerstrasse 3, 80335 Munich, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Tel. +49 611 973150, Web: www.euromarcom.de, E-Mail: team@euromarcom.de

Original content of: Horizon3.AI Europe GmbH, transmitted by news aktuell
Diese Meldung kann unter https://www.presseportal.de/en/pm/163532/6174776 abgerufen werden.