Study Warns on "Head-in-the-Sand" Approach to Cybersecurity

Wednesday 5 February, 2025

- **“Cyber Security Report 2024/2025” by Horizon3.ai for the United Kingdom**

- **Cybersecurity expert Keith Poyser: "Half of companies neglect regular assessments of their operational cyber risks, despite it being essential to protect themselves from potential threats and comply with modern legislation."**

At least half of UK organisations are neglecting to assess their operational cyber risks, despite the increasing threats in the cybersecurity landscape and the requirements of regulations such as DORA and NIS2, according to Keith Poyser, Vice President for EMEA at cybersecurity company Horizon3.ai. He cites findings from Horizon3.ai's “Cyber Security Report 2024/2025”, which surveyed 150 UK organisations. The report reveals that only 23% of the companies regularly conduct risk assessments of their IT infrastructure to determine how vulnerable they are to cyberattacks.

Industry veteran Keith Poyser raises a key concern: "Regular assessment of operational cybersecurity is essential to meet both current and forthcoming legal requirements for IT security. This includes the Cyber Security and Resilience Bill, set to be introduced to Parliament this year, alongside European regulations like the Cyber Resilience Act (CRA), which also impact UK organisations working with EU partners. Moreover, ongoing evaluations are the only effective way to mitigate the potentially severe consequences of cyberattacks. Companies that neglect to assess their cyber resilience are knowingly putting themselves at considerable risk."

Cyber Resilience Requires Regular Maintenance

Nearly a third of organisations acknowledge their weaknesses in this area, according to the survey. While 31% currently do not conduct cyber risk assessments, they intend to address this gap in the future. However, 29% perform assessments only once a year, a quickly out-of-date snapshot, which is insufficient to stay ahead of evolving threats.

The government's *Cyber security breaches survey 2024** estimates that UK businesses had experienced approximately 7.78 million cyber crimes of all types within 12 months. "Limiting penetration testing, getting a true attacker’s perspective, of your computing and cloud environments to just once a year borders on negligence," warns Poyser. He offers a striking analogy: "It’s like taking your car for an MOT once every hundred years. It might survive the century, but the odds are far from being in your favour."

Head-in-the-Sand Policy on Cybersecurity

Related Sectors:

Business & Finance ::

Related Keywords:

Cybersecurity :: horizon3.Ai :: Organisation :: Study :: Cyber Resilience ::

Scan Me:

According to the study, 13% of companies do not test their defences against cyberattacks at all—leaving them to be "tested" only by an actual attack. Furthermore, 11% have no plans to change this approach in the future. The remaining respondents either saw no need for such measures, were unable to provide an answer, or stated in the survey: "We are not aware of any cyber risks."

Cybersecurity leader Poyser criticises "a widespread head-in-the-sand-approach to cybersecurity" in many organisations. He explains: "Businesses install common defensive devices like firewalls, Endpoint Detection and Response (EDR), Cloud Native Application Protection Programmes (CNAPPs), and similar defensive security tooling, then simply rely on them to keep all types of attacks away from their environments. Penetration tests to assess the effectiveness of these measures are rarely carried out." This could explain why 23% of the organisations surveyed admit they have no idea whether they have suffered a cyberattack in the past two years.

From Defensive to Proactive: The Key to Cybersecurity Success

The survey reveals a concerning imbalance in cybersecurity strategies and suggests that the lack of preparedness in cybersecurity may stem from passive and uncertain approaches to security strategies. 34% of companies reported that they solely rely on defensive measures without actively testing their resilience, while 21% at least conduct occasional offensive exercises. Only 7% regularly engage in structured Red and Blue Team testing, and 15% recognise the need for offensive security but lack the know-how to implement it. Meanwhile, 18% delegate these crucial tasks to external consultants. This reactive mindset leaves many organisations exposed to potential cyber threats.

This reliance on external expertise extends to risk assessments as well. Among companies that conduct annual or periodic evaluations, 16% handle them in-house, while 42% bring in external service providers. A pentest involves a full-scale simulated cyberattack on a company’s IT infrastructure to test its resilience against real-world threats. As US cybersecurity expert Bruce Schneier aptly put it, "You can't defend. You can't prevent. The only thing you can do is detect and respond."

Cybersecurity expert Poyser confirms: "The UK economy relies far too heavily on the assumption that defense systems will work when needed, without systematically verifying their effectiveness. We need to shift from a defensive to a more proactive offensive approach to tackle cybersecurity crises."

* https://ots.de/pTA7ra

About Horizon3.ai and NodeZero: Horizon3.ai provides a cloud-based platform, NodeZero, enabling organisations and public authorities to simulate self-attacks on their IT infrastructure to assess their cyber resilience through penetration testing (pentesting). Thanks to its cloud model, the platform offers affordable, regular pentesting, making it accessible to mid-sized companies. Horizon3.ai continuously monitors the cybercrime landscape to ensure that newly discovered vulnerabilities are swiftly integrated into the cloud system. NodeZero not only identifies security flaws but also offers tailored recommendations for remediation. Through this platform, Horizon3.ai helps organisations meet rising regulatory demands for cyber resilience in Governance, Risk & Compliance (GRC), with guidelines recommending an internal self-attack at least once a week.

Trademark notice: NodeZero is a trademark of Horizon3.ai

Further information:
Horizon3.AI Europe GmbH, Sebastian-Kneipp-Str. 41, 60439 Frankfurt am Main, Web: www.horizon3.ai

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

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