Cybersecurity is a Boardroom Imperative: New Data Reveals Urgency for Proactive Defence

Monday 30 June, 2025

Related Sectors:

Business & Finance :: Computing & Telecoms ::

Scan Me:

- **Cyberattacks can cause significant financial losses, operational downtime, and lasting damage—making cybersecurity a growing boardroom priority.**
- **CEOs and executives are under increasing scrutiny from regulators, investors, and customers to demonstrate active oversight and risk management.**
- **Recent findings from Horizon3.ai's *Cybersecurity Report UK 2024/25* show that 62% of UK organisations that fell victim to cyberattacks experienced downtime, with 54% facing ransom demands and 35% having their data stolen.**
- **Proactive cybersecurity measures, such as continuous penetration testing, are essential for staying ahead of evolving cyber threats and safeguarding organisations from costly breaches.**

London, 30 June 2025 – Cyberattacks today have consequences that extend far beyond temporary disruption. As recent large-scale breaches in the retail sector have demonstrated, a single incident can trigger widespread operational outages, severe financial losses, and long-lasting reputational damage. With the scale and sophistication of these attacks continuing to grow, the pressure on executive leadership is mounting. CEOs, board members, and senior decision-makers are now expected—by regulators, stakeholders and customers alike—to take a more proactive role in managing cyber risk and ensuring their organisations are prepared to respond effectively.

"As attacks become more relentless, automated, and difficult to detect—and as regulatory expectations intensify—the responsibility of business leaders to protect sensitive systems and data has never been more urgent," said Keith Poyser, Vice President for EMEA at cybersecurity company Horizon3.ai.

The Economic Shockwaves of Cyberattacks

According to the *Cybersecurity Report UK 2024/25* by Horizon3.ai, which surveyed 150 organisations across the United Kingdom, nearly two-thirds reported experiencing at least one cyberattack in the past year. Among those affected, 62% suffered outages or downtime, 54% faced ransom demands, 42% experienced disruption to business operations, and 35% had data stolen—underscoring the wide-ranging and severe consequences of cyber incidents that contribute directly to rising financial costs.

Recent attacks on major UK retailers such as Co-op and M&S illustrate the real-world impact of these trends. In a public statement, the UK Cyber Monitoring Centre classified these incidents as "Category 2 systemic events". The breaches are estimated to have caused combined losses of up to £440 million, including legal costs, business interruption, incident response, reputational damage, and customer remediation. In response, cybersecurity experts have warned of a potential fraud surge across the UK. The incidents have also triggered heightened scrutiny from regulators and renewed calls for businesses to prioritise proactive cyber resilience.

When asked to estimate the total economic damage caused by cyberattacks across the UK, respondents to the *Cybersecurity Report UK 2024/25* offered a sobering range: 41% estimated losses between £1–50 billion, while others projected figures as high as £300 billion. While opinions varied, recent industry data suggests the actual financial impact may already exceed £44 billion over the past five years—a figure that signals just how widespread, costly, and escalating the threat of large-scale cyberattacks has become.

Proactivity and Testing: The Key to Cybersecurity Defence

As the scale and complexity of cyberattacks continue to grow, even well-resourced organisations are finding it increasingly challenging to defend against evolving threats. These pressures are exposing the limitations of traditional, reactive security approaches, which often rely on scheduled risk assessments and static controls. To address this, organisations must adopt offensive security—a proactive approach that uses real-world cyberattack techniques to uncover and address weaknesses before they can be exploited.

"An essential strategy is continuous, autonomous penetration testing of IT infrastructures, which uses real-world cyberattack techniques to identify exploitable attack paths before threat actors can target them. Regular testing allows businesses to stay one step ahead of evolving threats and helps ensure their defences are capable of withstanding sophisticated cyberattacks", said security expert Poyser.

Techniques such as penetration testing, red teaming, and autonomous attack emulation allow organisations to assess their systems from an attacker's perspective. This enables teams to identify critical weaknesses, prioritise remediation efforts, and validate the effectiveness of their defences under realistic conditions.

Understanding the Growing Liability

It is crucial that the responsibility for cybersecurity does not rest solely with IT departments but becomes a central topic in the boardroom. Cybersecurity is no longer just a technical issue; it is a business-critical concern that impacts revenue, reputation, regulatory compliance, and resilience. Senior leadership must be actively involved in shaping and driving the company's cybersecurity strategy to ensure comprehensive protection across all levels.

Cybersecurity is increasingly viewed as a legal and compliance matter. While UK law does not routinely assign personal liability to executives for cyber incidents, frameworks like the Network and Information Systems Directive 2 (NIS2) and the Digital Operational Resilience Act (DORA) are introducing stronger expectations for board-level governance—particularly for businesses in critical infrastructure and financial services. These frameworks emphasise the role of leadership in ensuring adequate security measures are in place and require boards to demonstrate oversight of risk management processes.

"UK companies working with EU partners must recognise that they are bound by these regulations. With the increasing frequency and severity of cyberattacks, it is anticipated that more such legislation will be introduced. Organisations are strongly encouraged to act now, learn from the missteps of others, and take proactive steps to avoid the potentially severe consequences down the line."

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.

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

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