Resilient Organisations Practise Until Response Becomes Routine, Says Horizon3.ai

Tuesday 3 March, 2026

Dan Bird MBE, Field Chief Technology Officer (EMEA) at Horizon3.ai, highlights why cyber resilience must move beyond policy and toward continuous operational rehearsal — reinforcing insights from co-founder and CEO Snehal Antani.

London – Cyber resilience is often framed as a new challenge driven by modern threats, yet many of its core lessons were already solved decades ago in disaster recovery. According to Dan Bird MBE, Field Chief Technology Officer (EMEA) at cybersecurity company Horizon3.ai, resilient organisations succeed not through static defence models but through continuous rehearsal and validation — an approach strongly echoed by Horizon3.ai co-founder and CEO Snehal Antani.

Bird points to a growing gap between policy and real-world readiness. Horizon3.ai, regarded as one of the leading providers of offensive security, promotes an approach in which organisations test their own IT environments through continuous penetration testing to uncover potential weaknesses that cybercriminals could exploit. Rather than solely relying on passive layers of defence, organisations can safely hack themselves, fix their issues, validate their fixes, and repeat the process as often as they like.

Parallels between cyber resilience and high availability systems

Drawing on Antani's comparison between cyber resilience and business continuity, Bird emphasises that resilience is not a theoretical concept but an operational discipline. In high availability environments, downtime is not acceptable and failures are anticipated rather than avoided. Systems are intentionally failed over from one data centre to another to prove recovery works, building the kind of repetition and accountability that creates "muscle memory" within teams.

This model of continuous rehearsal for real events aligns closely with offensive security principles and reflects what both Antani and Bird see as the most effective modern response to escalating cyber threats. Instead of viewing cyber resilience as a tooling or reporting exercise, Horizon3.ai argues that organisations must treat it as an operational challenge: systems fail, attackers exploit weaknesses, and businesses must recover under pressure. "Customers expect availability, and regulators demand accountability," said Bird.

Resilient organisations practise until action becomes routine

Bird reinforces Antani's view that resilient organisations should assume something will go wrong and actively look for weak points before attackers do. "Resilience means rehearsing response and recovery until execution becomes routine, whereas many organisations still rely on assumptions," he explained. "Defence and recovery plans may appear strong on paper but often fail in practice when testing is missing."

In real incidents, he notes, operational failures and malicious activity can appear indistinguishable at first. Service restoration cannot wait for perfect attribution. Disaster recovery and cybersecurity converge, requiring teams that have rehearsed together rather than siloed plans that have never been exercised under pressure. The challenge, Antani has argued, is rarely tooling alone but often process and leadership.

One penetration test a year is far too little

Both leaders highlight the limits of traditional annual penetration testing in environments that change constantly. Risks evolve faster than yearly cycles can capture, with patches arriving weekly, configurations shifting and cloud and identity architectures continuously developing. Without regular security validation, organisations risk making decisions based on outdated assumptions.

Bird emphasises that continuous testing tied closely to change creates the feedback loops organisations need. Regular pentests following patch cycles help teams validate whether improvements actually reduce risk, moving security toward continuous improvement rather than periodic assessment.

A new phase of cybersecurity driven by artificial intelligence

Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

horizon3.AI Europe GmbH :: Cyber Resilience :: Technology :: Dan Bird ::

Scan Me:

As Antani has observed, cybersecurity has entered a phase where speed matters more than ever. AI-driven attacks compress timelines, meaning organisations must rely on trained muscle memory rather than reactive decision-making. From Bird's perspective, the lesson is clear: "Under pressure, teams fall back on training, not expectations. Continuous rehearsal, combined with leadership commitment, determines performance."

Media enquiries & interview opportunities

Dan Bird MBE is available for interviews, expert commentary and contributed opinion pieces on cyber resilience, offensive security and the impact of AI-driven threats on critical infrastructure and national security.

Journalists interested in speaking with Dan can contact:

Tabea Dripke

euromarcom public relations

tabea@euromarcom.com

About Horizon3.ai.

Horizon3.ai's NodeZero® platform is trusted by 40% 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.

Editor's note: This announcement expands on themes discussed in an opinion article by Snehal Antani published in SC Media

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

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