Overconfident Organisations Prone to Cyber Breaches, Study Finds

Research from Adarma examines critical aspects of cybersecurity operations and reveals that overconfidence could leave businesses vulnerable to attack.

EDINBURGH, UNITED KINGDOM, September 12, 2023 /EINPresswire.com/ -- Adarma, an independent leader in detection and response services, published a report titled "A False Sense of Cybersecurity: How Feeling Safe Can Sabotage Your Business." The report examines critical aspects of security operations like confidence levels, 'tool sprawl', the use of artificial intelligence and the productivity and well-being of security teams.

> "More tools do not guarantee protection if they are not properly configured and talking to each other or, for example, if organisations don't have the expertise to manage incoming alerts appropriately."
>
> *John Maynard, CEO at Adarma*

Based on a survey* of 500 cybersecurity professionals from UK organisations with over 2000 employees, Adarma found that 95% of UK enterprises are 'very confident' (53%) or 'somewhat confident' (42%) that they do not have gaps in their security controls coverage. Yet, two-thirds (68%) have fallen victim to a cyber-attack in the last two years.

One possible reason for this disconnect could be the belief that having more security tools leads to better protection for the organisation. The research indicated that confidence levels tended to rise alongside the number of security tools used, as did the chances of experiencing a security breach.

Commenting on the report, Scott McElney, CISO of the Weir Group, cautioned against the assumption that more tooling leads to enhanced security, noting that "adding more tools may increase risk due to the complexities involved in managing them and the requisite skills needed to configure and optimise them."

The UK government's 2023 cybersecurity sectoral analysis reveals that there are currently 1,979 firms offering cybersecurity products and services in the country. However, 61% of respondents find this fragmented technology landscape hinders their ability to improve their security capabilities and performance. As a result, 80% are currently consolidating their security technology or plan to do so, and an additional 18% acknowledge the need to reduce their

tooling.

“Unfortunately, the proliferation of cybersecurity products and services has misled many into believing that they are the cure-all to our cybersecurity woes; in fact, it has introduced more complexity and confusion. More tools do not guarantee protection if they are not properly configured and talking to each other or, for example, if organisations don’t have the expertise to manage incoming alerts appropriately. Ultimately, technology is only as good as the people who are deploying, integrating and optimising it,” said John Maynard, Adarma’s CEO.

“By consolidating the tech stack, organisations stand to gain greater visibility over their application estate, allowing for more effective resourcing, more centralised competencies, and reduced digital fragmentation. But again, successfully making that transition without compromising the organisation’s cyber resilience comes down to having the right people with the know-how,” Maynard concludes.

Organisations encounter various difficulties when attempting to consolidate their technology stack. According to the survey, 45% struggle with implementation due to its complexity and the need for expertise. Another 43% mention the difficulty in optimising and utilising technology to its fullest potential. Additionally, 40% express concern about becoming dependent on a single vendor.

Adarma recommends that organisations adopt a comprehensive approach to security by considering the complete security technology lifecycle, as well as the required individuals and procedures for integration, configuration, and optimisation. Sufficient resources and capabilities should be assigned to effectively manage security tools.

Additionally, prioritising the consolidation of the security stack can improve efficiency and visibility. However, Adarma warns organisations should proceed cautiously by defining desired business outcomes and having an independent security architect lead the consolidation project.

Security leaders must trust both people and technology, acknowledge gaps in controls, and avoid overconfidence in security.

Read the full report here: www.adarma.com/a-false-sense-of-cybersecurity

*The survey was completed between the 15th and 22nd of May 2023.

Lara Joseph
Eskenzi PR
+44 7854 841892
lara@eskenzipr.com
Visit us on social media:

Twitter
LinkedIn
