Over Half of Organisations Are at Risk of Cyberattack Due to Exhausted and Stressed Staff

Research from Adarma finds that wellbeing and diversity continue to be at the forefront of cyber professionals' minds and crucial for the future of the industry

EDINBURGH, SCOTLAND, November 22, 2023 /EINPresswire.com/ -- Research from Adarma, an independent leader in detection and response services, has revealed that organisations believe that they are at significant risk of cyberattack due to stressed and exhausted staff. The report, entitled "A False Sense of Cybersecurity: How Feeling Safe Can Sabotage Your Business," highlights the worry faced by cybersecurity professionals when it comes to security, the skills shortage, and poor wellbeing.

Based on a survey* of 500 cybersecurity professionals from UK organisations with over 2000 employees, Adarma found that over half (51%) of organisations believe their security operations staff are challenged, stressed, frustrated and/or exhausted, so it's only a matter of time before mistakes are made, and some are burnt out and ready to quit. At a time when the cybersecurity industry already struggles significantly with talent acquisition and retention, organisations cannot afford to lose staff to burnout.

The findings also reveal the importance and value of diversity in cybersecurity recruitment. Optimistically, two-thirds (66%) believe recruiting from a wider, more diverse talent pool would offer significant help with the cybersecurity skills shortage. Additionally, 35% would consider working with a third-party provider for diversity strategies and to benefit from a more diverse team of talent. In fact, nearly two-thirds (61%) of cybersecurity professionals believe that a lack of different perspectives and diverse representation is holding them back.

"Cybersecurity professionals are typically highly passionate people, who feel a strong personal sense of duty to protect their organisation and they'll often go above and beyond in their roles. But, without the right support and access to resources in place, it's easy to see how they can quickly become victims of their own passion. The pressure is high and security teams are often understaffed, so it is understandable that many cybersecurity professionals are reporting frustration, burnout, and unsustainable stress. As a result, the potential for mistakes being made that will negatively impact an organisation increases. Business leaders should identify opportunities to ease these gaps, so that their teams can focus on the main task at hand, protecting the organisation," said John Maynard, Adarma's CEO.

The security risk posed by a lack of skills, diversity, and the prevalence of poor mental health among cybersecurity teams exemplifies the real-world effects of burnout and talent shortages. The research revealed that over 40% of cybersecurity leaders feel like they have limited capabilities and expertise to fully understand the threats they face, while a further 43% say that they have some, little or no capabilities or expertise to detect and respond to potential threats in their IT environments. Concerningly, one in four (25%) respondents stated that they have limited capability or expertise to respond effectively to an incident at all.

"One of the best things that can be done for team capability and performance is to fill it with diverse and thoughtful individuals. By diversifying the talent pool, new ideas flow and various perspectives can pave the way for innovation. Exploring non-traditional recruitment paths will help to further widen that talent pool by making careers in cybersecurity more accessible to a broader range of candidates. This could go a long way to easing the burden on overworked security teams while also providing opportunity for growth. Indeed, the well-being of the entire workforce, including the security department, must be prioritised and requires the right balance of reliance on technology and people. Ultimately, we want to see organisations strengthen their security defences, optimise resource allocation and invest in people's capabilities. This will produce a strong overall security posture that can effectively protect against the evolving threat landscape." Maynard added.

Based on these findings, Adarma's report concludes with recommendations for security leaders and teams to enhance an organisation's overall cybersecurity posture. The survey revealed that 28% of cybersecurity professionals believe their capacity for innovation is limited, with 60% attributing a major reason for being held back to the skills shortage. However, there are actionable ways for security teams to strengthen themselves. These include consolidating the security stack to improve efficiency, regularly reviewing security tool configurations, leveraging automation and AI and investing in the support of cybersecurity professionals' wellbeing.

Adarma empowers security leaders to increase diversity, foster inclusivity, and ease the burden on their teams.

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
+447854841892 ext.
lara@eskenzipr.com
Visit us on social media:
Twitter
LinkedIn