PROJECT MANAGEMENT GLOBAL
The Place for People in Projects

Cybersecurity Teams Strained by Understaffing and Underfunding

October 7, 2024

A new report by ISACA, the leading global professional association for IT governance and cybersecurity, reveals that cybersecurity teams are under immense pressure due to understaffing and underfunding.

The report, based on a survey of European cybersecurity professionals, found that 61% of organizations are facing a shortage of cybersecurity staff and over half (52%) believe their cybersecurity budgets are inadequate. These staffing and funding struggles are taking a toll on the well-being of cybersecurity professionals, with 68% reporting increased stress levels compared to five years ago.

The increasingly complex threat landscape is a major contributor to this stress, with two in five respondents (41%) experiencing more cyberattacks in the past year. Over half (58%) expect their organizations to face cyberattacks in the next year, highlighting the urgent need for investment in skilled cybersecurity teams.

Chris Dimitriadis, Chief Global Strategy Officer at ISACA, said: *"In an increasingly complex threat landscape, it is vital that, as an industry, we overcome these hurdles of underfunding and under-staffed teams. Without strong, skilled teams, the security resilience of whole ecosystems is at risk – leaving critical infrastructure vulnerable."*

Despite the need for skilled teams to protect businesses, 19% say that their organisation has unfilled and open entry-level positions available, and 48% have unfilled open positions which require experience, a university degree, or other credentials. These figures have dropped only a few percentage points (from 22% and 53%) since 2023, pointing to an ongoing struggle to fill open positions.

52% of respondents say that soft skills are lacking the most amongst today's cybersecurity professionals. Of the soft skills in question, 54% feel that communication skills (e.g. speaking and listening skills) are most important, followed by problem-solving (53%) and critical thinking (48%).

Dimitriadis added: *"The cybersecurity industry will massively benefit from a diverse range of people – each with different skills, experiences, and perspectives. This is the key to plugging the skills gap. Once talent enters the industry, businesses can then train and upskill new entrants on the job with cyber certifications and qualifications."*

Mike Mellor, Vice President, Security Engineering at Adobe, who sponsored the research, said: *"With the increasing frequency and sophistication of cyberattacks, it's essential for organisations to adopt secure authentication methods to strengthen their defences. Adobe believes that fostering a deep security culture among all employees through anti-phishing training, combined with stronger controls such as zero-trust*

networks protected by phishing-resistant authentication are essential in safeguarding any organisation."