Two-Thirds of Organizations Have Unfilled Cybersecurity Positions

Data: 2025-09-29 11:15:00

Autor: Inteligência Against Invaders

Organizations continue to experience significant cybersecurity skills shortages, with 65% of firms

reporting unfilled cyber positions, a new ISACA survey has found.

Over a third (38%) of cybersecurity professionals surveyed revealed it takes three to six months to hire for entry-level roles and 39% said the same for non-entry-level positions.

Additionally, half of organizations admitted that they struggle to retain cyber talent.

In total, 55% of respondents believe their security teams are understaffed. This represents a small drop from 2024, when 61% said their team is understaffed.

Over half (53%) of respondents believe their cybersecurity budget is underfunded, which is down from 59% in 2024. However, fewer expect their budget to increase compared to last year's State of Cyber 2025research (41% vs. 47%).

Just 56% think that their board prioritizes cybersecurity.

Chris Dimitriadis, chief global strategy officer at ISACA, commented: "While organizations are starting to acknowledge the problem and take steps to address long-standing issues in budgets and staffing, the pace of change is still far too slow."

He added: "The reality is that cybercriminals are moving faster than most organizations can respond. Now is the time to invest in investing in a more holistically trained cybersecurity workforce, an investment towards customer trust and in gaining competitive advantages, not just a reactive move following an incident."

University Graduates Unprepared for Cyber Roles

Just 27% of respondents believe university graduates are well prepared for cybersecurity roles.

The top knowledge gaps in new graduates included incident response (43%), data security (39%), threat detection and response (39%) and identity and access management (39%).

Security professionals emphasized the need for more soft skills in their teams ahead of formal qualifications, with 59% reporting a gap in this area. The top three soft skills required were critical thinking (57%), communication (56%) and problem solving (47%).

Adaptability was considered the top qualification factor for security roles (61%), followed by hands-on experience (60%).

Overall, 46% of those surveyed said that more than half of their cyber team transitioned into the field from other roles.

Dimitriadis said the findings demonstrate the need to keep widening the pathways into the cybersecurity sector.

“By valuing hands-on training, professional credentials and transferable skills, organizations can strengthen their teams and ease the pressure on overstretched professionals,” he noted.

Threat Landscape Increasing Pressure on Cyber Pros

The ISACA research also highlighted growing pressures on cybersecurity professionals. Around two-thirds (66%) said their role is more stressful than five years ago.

The biggest contributing factor is the complex threat landscape, cited by 63% of respondents.

Over a third (35%) reported increased attacks in 2025, while 43% believe an attack on their organization is likely or very likely in the next year.

Additionally, 39% believe that cybercrime is underreported, even when reporting is required by law.

Just 41% said they are confident in their team’s incident-response capabilities.

The top attack vector cited by respondents was social engineering (44%). This was followed by exploited vulnerabilities (37%) and malware (26%).

ISACA’s *State of Cybersecurity 2025-2026* report surveyed more than 3800 cybersecurity professionals globally.