New ISACA study finds cybersecurity leaders face global hiring challenges contributing to staff gaps and increased cyber-attacks

State of Cybersecurity 2021 report finds 61 percent of cybersecurity teams are understaffed

Sydney, Australia (5 May 2021) – ISACA has released its annual State of Cybersecurity 2021 survey report which reveals concerning trends around hiring and staff retention continue in the cyber workforce. The global study of more than 3,600 cyber security leaders reports consistent challenges finding qualified, well-rounded candidates, while understaffed teams remain strongly correlated to an increasing number of cyber-attacks.
Positively, the cybersecurity workforce was largely spared the pandemic devastation experienced by other sectors, but the survey found that longstanding issues persist.
Respondents in Australia and New Zealand report similar views to their global colleagues including:
66% of respondents indicate that their cybersecurity teams are understaffed (61% globally). 59% say they have unfilled cybersecurity positions (55% globally). 52% say their cybersecurity applicants are not well qualified (50% globally). Only 35% say HR regularly understands their cybersecurity hiring needs (31% globally). Additionally, soft skills remain the biggest skills gap according to 68% of respondents in Australia and New Zealand followed by security controls (34%) and data related areas (33%).
The results also show that 59% of respondents in Australia and New Zealand had difficulty retaining talent last year during the pandemic citing the top three reasons for staff leaving as being recruited by another company (64%), lack of financial incentives (56%) and limited promotion and development opportunities (51%).

Staff Gaps and Attacks Linked
As in years past, the findings show that retention issues and increased cyberattacks are somewhat interrelated. Globally, 68% of respondents who experienced more cyberattacks in the past report being somewhat or significantly understaffed, and 63% who experienced more cyberattacks in the past indicated they have experienced difficulties retaining qualified cybersecurity professionals.

“It has become even more evident in the past year just how vital cybersecurity is to ensuring business continuity, yet the years-long struggle to staff these teams continues,” said Jonathan Brandt, ISACA information security professional practices lead. “As a global cybersecurity community, it is imperative that we all come together to recalibrate how we hire, train and retain our future cyber leaders to ensure we have a solid workforce to meet these evolving cybersecurity needs.”

Hiring and Skills Challenges Persist, Especially with Recent Graduates
Despite the high demand for cybersecurity jobs, 50% of those surveyed globally generally do not believe that their applicants are well qualified. Additionally, only 27% of all survey respondents say that recent graduates in cybersecurity are well-prepared, though 58% indicate that they require a degree for entry-level cybersecurity positions. Global respondents note that they also seek prior hands-on cybersecurity experience (95%), credentials (89%) and hands-on training (81%) when determining whether a candidate is qualified. Organisations are addressing these challenges by:

Training non-security staff who are interested in moving to security roles (43%)Increasing usage of contract employees or outside contractors (37%)Increasing use of reskilling programs (23%)Increasing use of performance-based training to build hands-on skill (22%)Increasing reliance on AI/automation (22%)
“Making a meaningful difference in addressing the persistent skills gaps in the cybersecurity workforce will require a collaborative and concerted effort between government, academia and industry,” says Renju Varghese, Fellow & Chief Architect, CyberSecurity & GRC Services, HCL Technologies. “Through strategic partnerships and outreach, we will be able to not only better prepare graduates coming out of university programs but also equip a wide range of candidates from non-traditional paths with the skills needed to succeed in a cybersecurity career.”

David Samuelson, ISACA CEO, said ISACA is not only committed to providing research and best practices to guide its global professional community, but also by taking action to help fill the skills gap. “This includes transforming our digital and learning tools to give individuals and companies training that is more relevant and customised than ever before and supporting the important work of the One In Tech foundation in advancing equity and inclusion in the tech workforce.”

For a complimentary copy of State of Cybersecurity 2021 Part 1, insights from industry leaders and related resources,

visit www.isaca.org/state-of-cybersecurity-2021.

###

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organisations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organisation that leverages the expertise of its more than 150,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

Twitter: www.twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews

Contact:
Karen Keech, karen@establishedmedia.com, 0411 052 408

Contacts

Karen Keech
0411 052 408
mailto: