ISACA research explores how AI security solutions are being deployed to address the cybersecurity skills gap

ISACA's State of Cybersecurity 2020 Part 2 survey highlights the role of AI in combatting cyberattacks and discusses the impact of cyberattacks on cloud-based service providers.

Sydney, Australia (10 June 2020) – Thirty per cent of survey respondents are using artificial intelligence (AI) and machine learning tools in their security operations to combat cybercrime, according to ISACA's State of Cybersecurity 2020 Survey Part 2 report. While adoption is still relatively low, despite the numerous products now available in the marketplace, early indications suggest these solutions provide increased visibility, with respondents better able to quantify attack rates. Additionally, the use of AI is one of the top four ways in which organisations are tackling the cybersecurity skills gap, ranking just behind performance-based training of cybersecurity staff. "As senior leadership and crisis management teams plan for the new normal, cybersecurity is a key discussion point. Though the use of AI in mitigating the cybersecurity skills gap is still not yet widely adopted, we expect implementation of AI security solutions to increase, as these strategies are increasingly proven beneficial across various industries," says Ed Moyle, founding partner, Security Curve, and lead writer of the report. The ISACA report also highlights the increased use of cloud-based software and how the threat landscape may change as a result. Enterprises continue to embrace software-as-a-service (SaaS) applications for critical business activities and continue to look to platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) solutions to bolster or replace internally hosted resources. "As resources continue to move externally, a shift in the number of attacks from end-user computing environments to cloud services providers is probable," says Jo Stewart-Rattray former ISACA board director and Director of Information Security & IT Assurance, BRM Advisory. "This may also lead to a decrease in an enterprises' visibility into the type and number of cyberattacks, as attacks are counted and managed by the cloud provider's security operations team." Cybercrime still underreported This year's report found the top attack types as social engineering (15%), advanced persistent threat (10%) and ransomware and unpatched systems (9% each). Yet, respondents believe that cybercrime remains underreported, with 62% of professionals believing that enterprises are failing to report cybercrimes, even in situations where they have a legal or contractual obligation to do so. This trend, highlighted in last year's report, continues unabated. Worryingly, as some regulations carry a penalty for failure to report, this data suggests many organisations are knowingly or unknowingly taking on regulatory risk. Additionally, as 53% of respondents report that the board of directors has adequately prioritised cybersecurity, it would be expected that the security function would therefore be integrated into enterprise governance. The fact that the perception of underreporting continues given strong coordination with other departments and implicit oversight implies a systemic failure to report. "These findings also reveal some hard truths our profession needs to face around the need for greater transparency and communication around these attacks, so that practitioners can fully understand and effectively respond to the current threat landscape they are facing," adds Moyle. The survey, with responses from more than 2,000 respondents from over 17 industries and 102 countries, found cyberattacks are also continuing to increase, with 32% of respondents reporting an increase in the number of attacks relative to a year ago. To read the full report, expert insights and related resources, visit: www.isaca.org/state-of-cybersecurity-2020. More resources around cybersecurity can be found at www.isaca.org/training-and-events/cybersecurity. ### 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 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including 223 chapters worldwide.
Twitter: www.twitter.com/ISACANews LinkedIn: www.linkedin.com/company/isaca Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews Contact: Julie Fenwick, jfenwick@daylightagency.com.au, +61 468 901 655 Karen Keech, kkeech@daylightagency.com.au, +61 411 052 408

Contacts

Julie Fenwick
The Daylight Agency
mailto:
Karen Keech
0411 052 408
mailto: