Artificial Intelligence (AI) Initiatives Driving Increased Focus on Cybersecurity, According to New Rackspace Technology Survey, in Association with Microsoft

September 19, 2023

AI seen as both potential vector for cyberattacks and enabler of resiliency; Organizations prioritize investment in cloud-native security but lack internal expertise

SAN ANTONIO, Sept. 19, 2023 (GLOBE NEWSWIRE) -- New global cybersecurity research by Rackspace Technology (NASDAQ: RXT), a leading end-to-end, multicloud technology solutions company, conducted in association with Microsoft, finds that artificial intelligence (AI) is playing an increasingly critical role in driving organizations' security postures and their need for investment in cybersecurity. When asked how AI is influencing their organization's security posture, 62% of survey respondents said that AI has increased their need for cybersecurity, resulting in stricter security measures on data storage and access (58%), greater attention to the exposure of sensitive data (52%) and stronger classification frameworks and guidelines (47%).

At the same time, survey respondents say that AI-enabled technologies have become a critical tool in the security arsenal across several cyber investment areas, including app security (85%), cloud-native security (84%), and data security (81%). 81% also say their organizations have a formal policy in place on AI governance and security, though only 39% say that the level of awareness and understanding among employees of their policy is "great," vs. 43% who characterize it as "fair."

"As AI has emerged as an increasingly important area of focus for organizations of all sizes, it presents both challenges and opportunities for security teams," said Jeff DeVerter, Chief Technology Evangelist, Rackspace Technology. "We are seeing an increased focus on AI data governance and a heightened focus on cloud-native security as organizations' infrastructures become more distributed and the IT perimeter blurred. But we are also seeing more companies leveraging AI to fight attackers and stay ahead of the curve while prioritizing personnel training to help them better understand and avoid vulnerabilities."

Cyber budgets rise, with cloud architecture attacks a leading concern
62% of survey respondents say they have increased their cyber budget over the past year, while only 3% said they have made cuts. Meanwhile, 33% of those who have increased say they have raised their cybersecurity budget by more than 14%. 48% of surveyed organizations say they dedicate more than 14% of their total IT budget to cyber. The biggest areas of investment are cloud-native security (57%), data security (51%), and application security (48%), which saw a 7% increase over Rackspace's 2022 survey.

One major factor driving the increase is the rise in concern over cloud architecture attacks, which rose 12% compared to 2022 and which 62% of respondents identify as their biggest threat. It is also the area organizations feel the least prepared to address themselves, with 49% relying on a partner to deliver cloud-native security.

Continuing talent crunch leads to more partnering
Securing and retaining cybersecurity talent remains a major organizational hurdle, with survey respondents identifying a shortage of skilled workers as their leading cyber challenge. In an ultra-competitive hiring environment with high employee turnover, companies are more reliant than ever on outside partners rather than bringing on additional internal resources. 43% of respondents cite engaging with cybersecurity services partners for consultation or support as a top three priority, with a lack of internal expertise being the leading cause.

"As cybersecurity has become increasingly complex, with workloads and data deployed across multiple platforms, it has become much more difficult to maintain a 'go it alone' mentality," said D K Sinha, President, Public Cloud for Rackspace Technology. "Fortunately, there is a plethora of great cloud security tools available to organizations and partner networks that can help fill in knowledge gaps."

Stronger C-suite and board engagement
Engagement of C-suites and boards with the array of cyber threats they face is positively impacting visibility, buy-in, and collaboration. According to the survey, cybersecurity remains the top concern for the C-suite (63%) – above issues such as digital transformation (57%), interest rates (48%), retaining/hiring employees (43%), and supply chain/logistics management (38%) – and up from 58% in Rackspace's 2022 survey. 69% of respondents say the level of concern for cybersecurity has increased in their C-suite over the past 12 months, while 71% say the C-suite is making more of an investment in cybersecurity. 65% also say that better collaboration between the security team and the C-suite has effectively reduced the cyber skills gap. Meanwhile, 70% of respondents say cybersecurity is a top two concern for their board of directors.

Click here for additional information about the global security research, including the survey whitepaper and infographic.

About Rackspace Technology

Rackspace Technology is a leading end-to-end multicloud technology services company. We can design, build and operate our customers' cloud environments across all major technology platforms, irrespective of technology stack or deployment model. We partner with our customers at every stage of their cloud journey, enabling them to modernize applications, build new products and adopt innovative technologies.

Survey Methodology

Commissioned by Rackspace Technology and Microsoft, Coleman Parkers Research conducted the survey between July 17, - August 20, 2023, based on the responses of 1,420 IT decision-makers across manufacturing, digital native/technology, financial services, retail, government/public sector, and healthcare sectors in the Americas, Europe, Asia, and the Middle East.

Media Contact: Natalie Silva, publicrelations@rackspace.com