New Rackspace Technology Survey of Global IT Leaders Reveals Lack of Confidence, Resources Within Their Organizations in Responding to Growing Array of Cyber Threats

October 20, 2021

Recruiting Challenges, IT Evolution and Remote Work Environments Among Factors Increasing Security Complexity

SAN ANTONIO, Oct. 20, 2021 (GLOBE NEWSWIRE) -- Half of global IT leaders say they are not “fully confident” in their ability to respond to data, malware phishing, supply chain, ransomware, cloud, IoT and application attacks, according to a new global survey by Rackspace Technology® (NASDAQ: RXT), a leading end-to-end, multicloud technology solutions company. Moreover, when asked about their attack response capabilities, fewer than half (45%) of respondents say they can effectively respond to incidents, mitigate threats (43%), or understand the nature of the threats they are facing (42%).

The survey of 1,420 IT professionals also reveals widespread uncertainty that organizations possess the talent and skills to meet cybersecurity challenges, with 86% of respondents saying their organizations lack the necessary skills and expertise to respond to a growing array of threats.

“Though most respondents to our survey say they are ‘prepared’ for cyber-attacks, there is a high degree of anxiety about their ability to effectively confront adversaries who are increasingly sophisticated,” said Jeff DeVerter, Chief Evangelist Rackspace Technology. “Moreover, the expanding use of the cloud, IoT and applications, as well as a tight talent market and an increase in remote work – largely driven by the pandemic – have made the security environment much more challenging. Few organizations actually have the people, processes, and technologies that match a modern cybersecurity model.”

IT Trends Driving Cyber Complexity

The ubiquity of the cloud, DevOps methodologies and the condensing of development cycles, coupled with other IT trends, have made addressing cyberthreats an increasingly complex task. Half of the survey respondents (49%) cite the growth in cloud and IoT as key challenges, followed by new threats and attack methods (46%) and the growth in data volumes, digital operations, and remote work (45%), which has resulted in increased opportunities for attackers.

Forty-eight percent of respondents say their ability to manage application security in a more complex environment is influenced by new ways of working, including DevOps and Agile development practices. Other dynamics include faster release/delivery cycles (46%), the growth in microservice application architectures (46%), hybrid/multicloud environments (46%) and container runtime environments (44%).

When asked about the nature and targets of the cyberattacks they are most concerned about, network/platform attacks (58%) lead the way, followed by web application attacks (52%) and network operating system attacks (51%). Half (50%) are concerned about Advanced Persistent Threats (APTs), while 47% involve stolen credentials and 41% are concerned about unauthorized exposure to data.

Talent and Staffing Pain Points

More than half (52%) of survey respondents say they have difficulty recruiting and retaining cybersecurity talent, with the greatest skill gaps in the areas of cloud security (33%) and network security (30%), which respondents also identified as their most critical roles. Across the business, IT leaders cite lack of expertise (86%), lack of resources (81%), lack of time (70%) and lack of training information (63%) as their most pressing cybersecurity and compliance challenges.

Cloud, data, app, network and identity access are most frequently handled by in-house staff while nearly half (49%) outsource integrated risk security and (43%) task external partners to assist with network security.

“Organizations struggling with expertise, resources and time are still reluctant about enlisting external help,” added DeVerter. “Instead, our research shows that they are hoping that enlisting recruiters and improving the training of internal staff will help them solve the talent crunch.”

Click here to view *How mature do IT leaders think they are when it comes to cloud security* Survey of Global IT Leaders Infographic.

How mature do IT leaders think they are when it comes to cloud security?

Survey Methodology
The survey was conducted by Coleman Parkes Research in September 2021. Findings are based on the responses of 1,420 IT decision-makers across manufacturing, retail, hospitality/travel, healthcare/pharma/biomedical, government and financial services sectors in the Americas, Europe, Asia and the Middle East. Most of the companies/organizations polled were founded before the year 2000, have from 101 to 999 employees, and annual revenue between $50m and $1b. They also have anywhere from two to 15 employees dedicated to cybersecurity and they spend 5% to 15% of their IT budget on cybersecurity.

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.

Contact:
Natalie Silva
Rackspace Technology Corporate Communications
publicrelations@rackspace.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/62925024-9e53-478b-9b06-acfc317c5543

Recruiting Challenges, IT Evolution and Remote Work