NEWS RELEASE

Cisco 2020 CISO Benchmark Report Shows Increased Investment in Cloud Security and Automation Technologies to Combat Complexity

2020-02-24

- Executive leadership still considers security a high priority along with other indicators such as clarification of roles, establishing clear metrics, and cyber risk assessments.
- Report shows increased challenges when managing and securing multi-vendor environments, cloud infrastructure, mobile devices, and unpatched vulnerabilities.
- 86 percent of security professionals say utilizing cloud security has increased visibility into their networks.

SAN FRANCISCO, Feb. 24, 2020 /PRNewswire/ -- **RSA Conference 2020** — Today, Cisco published its sixth annual CISO Benchmark Report surveying the security posture of 2,800 security professionals from 13 countries around the globe. The report provides 20 cybersecurity considerations for 2020 – gleaned from data analysis of survey results and a panel of Advisory CISOs.

Complexity Continues to be Cybersecurity's Worst Enemy
Digital transformation continues to present itself as an opportunity for IT and security leaders to innovate and gain competitive advantage. But it also carries a tsunami of infrastructure change, which often creates new challenges for security professionals with defeating unknown sophisticated threats looming as a top concern.

In today's security landscape, the average company uses more than 20 security technologies. While vendor consolidation is steadily increasing with 86 percent of organizations using between 1 and 20 vendors, more than 20 percent feel that managing a multi-vendor environment is very challenging, which has increased by 8 percent since 2017. Other notable findings:

- Forty-two percent of respondents are suffering from cybersecurity fatigue, defined as virtually giving up on proactively defending against malicious actors.
- Over 96 percent of fatigue sufferers saying that managing a multi-vendor environment is challenging, complexity being the main causes of burnout.

To combat complexity, security professionals are increasing investments in automation to simplify and speed up response times in their security ecosystems; using cloud security to improve visibility into their networks; and sustaining collaboration between networking, endpoint and security teams.

"As organizations increasingly embrace digital transformation, CISOs are placing higher priority in adopting new security technologies to reduce exposure against malicious actors and threats. Often, many of these solutions don't integrate, creating substantial complexity in managing their security environment," said **Steve Martino, Senior Vice President and Chief Information Security Officer, Cisco**. "To address this issue, security professionals will continue steady movement towards vendor consolidation, while increasing reliance on cloud security and automation to strengthen their security posture and reduce the risk of breaches."

The following findings highlight additional CISO challenges and opportunities for improvement:

- **Workload protection for all user and device connections across the network was found extremely challenging**—Forty-one percent of the surveyed organizations found data centers were extremely difficult to defend, and 39 percent said they struggled to secure applications. The most troublesome place to defend data was the public cloud, with 52 percent finding it very or extremely challenging to secure, and 50 percent claiming private cloud infrastructure was a top security challenge.
- **Security professionals struggle to secure the growing mobile workforce and ubiquitous personal devices** — More than half (52 percent) of respondents stated mobile devices are now very or extremely challenging to defend. Adopting zero-trust technologies can help secure managed and unmanaged devices without slowing down employees.
- **Adoption of zero-trust technologies to secure access of the network, applications, users, devices and workloads needs to increase**—Only 27 percent of organizations are currently using multi-factor authentication (MFA), a valuable zero-trust technology to secure the workforce. Survey respondents from the following countries showed the highest MFA adoption rates in this order: USA, China, Italy, India, Germany, and UK. While micro-segmentation, a zero-trust approach to secure access of workloads, had the least adoption at only 17 percent of respondents.
- **Breaches due to an unpatched vulnerability caused higher levels of data loss**— A key concern for 2020 is that 46 percent of organizations, up from 30 percent in last year's report, had an incident caused by an unpatched vulnerability. Sixty-eight percent of organizations breached from an unpatched vulnerability suffered losses of 10,000 data records or more last year. In contrast, for those who said they suffered a breach from other causes, only 41percent lost 10,000 or more records in the same timeframe.

Security professionals have made positive developments to improve their security posture:

- **Collaboration between network and security teams remains high**— Ninety-one percent of respondents reported they're very or extremely collaborative.
- **Security practitioners are realizing the benefits of automation for solving their skills shortage problem as they adopt solutions with greater machine learning and artificial intelligence capabilities**—Seventy-seven percent of our survey respondents are planning to increase automation to simplify and speed up response times in their security ecosystems.
- **Cloud security adoption is increasing, improving effectiveness and efficiency**— Eighty-six percent of respondents say utilizing cloud security increased visibility into their networks.

Recommendations for CISOs:

- Employ a layered defense, which should include MFA, network segmentation, and endpoint protection.

- Gain the highest levels of visibility to bolster data governance, lower risk, and increase compliance.
- Focus on cyber hygiene: shore up defenses, update and patch devices, and conduct drills and training.
- Implement a zero-trust framework to build security maturity.
- To reduce complexity and alert overload, adopt an integrated platform approach when managing multiple security solutions.

Additional Resources:

- Cisco 2020 CISO Benchmark Report
- Blog: A 2020 Vision for Cybersecurity by Steve Martino

Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at newsroom.cisco.com and follow us on Twitter at @Cisco.

Press contact: Raquel Prieto, raqpriet@cisco.com

View original content to download multimedia:http://www.prnewswire.com/news-releases/cisco-2020-ciso-benchmark-report-shows-increased-investment-in-cloud-security-and-automation-technologies-to-combat-complexity-301009684.html

SOURCE Cisco