NEWS RELEASE

Caution Security Startups, Investors, and Standalone Solutions--Cisco 2019 CISO Benchmark Study Reports Increased Vendor Consolidation

2019-02-28

Survey of 3200 security leaders shows increased investment in defense technologies, security training, risk analysis and risk mitigation, as the unknown in users, data, devices, and apps are a major concern for CISOs

SAN JOSE, Calif., Feb. 28, 2019 /PRNewswire/ -- In the run up to the world's largest cybersecurity show, the RSA conference, Cisco today published its fifth annual 2019 CISO Benchmark Study. The comprehensive survey of more than 3000 security leaders across 18 countries is an annual health check on the state of the CISO. This year's results show security professionals are placing higher priority on vendor consolidation, collaboration between networking and security teams, and security awareness exercises to strengthen an organizations security posture and reduce the risk of breaches. To further address complexity challenges, many CISOs are increasingly confident that migrating to the cloud will improve protection efforts, while apparently decreasing reliance on less proven technologies such as artificial intelligence (AI).

Complex security environments made up of solutions from 10 or more security vendors could be hampering security professional's visibility across their environments. Sixty-five percent of respondents do not find it easy to determine the scope of a compromise, contain it and remediate from exploits. The unknown threats that exist outside the enterprise in the form of users, data, devices, and apps is also a top concern for CISOs. To help address these challenges, and better protect their organizations, of those surveyed:

- Forty-four percent have increased investment in security defense technologies.
- Thirty-nine percent have security awareness training among employees.
- Thirty-nine percent focused on implementing risk mitigation techniques.

Survey respondents also noted the continued high financial impact of breaches. Forty-five percent of respondents reported the financial impact of a breach to their organization was more than $500,000. The good news is that more than 50 percent of respondents are driving breach costs below half a

million. But there remains a stubborn eight percent claiming an eye-watering cost of more than $5 million per incident for their most significant breach of the past year.

"This year, more than ever CISOs are taking a much more proactive role in reducing their exposure through consolidation and training, as well as investments in critical technologies, for cyber defense and breach containment, but there is still more to do," said **Steve Martino, Senior Vice President and Chief Information Security Officer, Cisco**. "You can't protect what you can't see, and security leaders are still struggling to gain greater visibility across their organization and into threats. Cisco is committed to helping organizations address these challenges and implement new techniques and technology to stay one step ahead of malicious actors and threats."

The following findings highlight some of these positive developments security professionals have made to improve their security posture:

- **The trend away from point products to vendor consolidation continues**— in 2017 54 percent of respondents cited 10 or fewer vendors in their environment. This number has risen to 63 percent.
    - In many environments, multiple vendor solutions aren't integrated, and therefore don't share alert triage and prioritization. The survey showed that even those CISOs with fewer point solutions could better manage their alerts through an enterprise architecture approach.
- **The most collaborative teams lose the least money. Elimination of silos shows a tangible financial upside**:
    - Ninety-five percent of security professionals reported that their networking and security teams were very or extremely collaborative.
    - Fifty-nine percent of those who stated that their networking and security teams were very/extremely collaborative also stated that the financial impact from their most serious breach was under $100,000 – the lowest category of breach cost in the survey.
- **There is more confidence in cloud-delivered security and in securing the cloud**.
    - Ninety-three percent of CISOs reported that migrating to the cloud increased efficiency and effectiveness for their teams.
    - The perception of difficulty of protecting cloud infrastructure has decreased—52 percent in 2019 compared to 55 percent in 2017.
- **Use of risk assessment and risk metrics that span across the business, in part driven by cyber insurance procurement, is playing an increasing role in technology selection and has helped CISOs focus on their operational practices**—40 percent of respondents are using cyber insurance, at least partly, to set their budgets.
- **"Cyber fatigue**" – defined as virtually giving up on staying ahead of malicious threats and bad actors - is down from 46 percent in 2018 to 30 percent in 2019.

But the fight is far from over--the following findings show CISO challenges and opportunities for improvement:

- **AI and machine learning (ML), used right, are essential to the initial stages of alert prioritization and management.** However, reliance on these technologies has decreased as respondents possibly perceive the tools to be still in their infancy or not ready for prime time:
    - Reliance on ML is down to 67 percent in 2019 compared to 77 percent in 2018.
    - AI is down to 66 percent compared to 74 percent in 2018.
    - Automation is down to 75 percent compared to 83 percent in 2018.
- **Employees/users continue to be one of the greatest protection challenges for many CISOs**

—having an organizational process that starts with security awareness training on day one is essential.
    - Only 51 percent rate themselves as doing an excellent job of managing employee security via comprehensive onboarding and processes for transfers and departures.

- **Email security remains the number one threat vector.**
    - Phishing and risky user behavior (e.g. clicking malicious links in email or websites) remains high and is the top concern for CISOs. The perception of this risk has held steady for the past three years between 56 to 57 percent of respondents. Coupled with low levels of security-related employee awareness programs, this represents a possible major gap that the security industry can help address.

- **Alert management and remediation remains challenging. A reported drop in remediation of legitimate alerts, 50.5 percent in 2018 to 42.7 percent this year, is concerning given that many respondents are moving toward remediation as a key indicator of security effectiveness.**
    - Security measurements are changing. The number of respondents who use mean time to detection as a metric for security effectiveness decreased from 61 percent in 2018 to 51 percent in 2019 on average. Time to patch has also dropped in focus from 57 percent in 2018 to 40 percent in 2019. Time to remediate has risen as a success metric: 48 percent of respondents cited this compared to 30 percent in 2018.

Recommendations for CISOs:

- Base security budgeting on measured security outcomes with practical strategies coupled with cyber insurance and risk assessments to guide your procurement, strategy, and management decisions.
- There are proven processes that organizations can employ to reduce their exposure and extent of breaches. Prepare with drills; employ rigorous investigative methods; and know the most expedient methods of recovery.
- The only way to understand the underlying security needs of a business case is to collaborate across siloes – between IT, Networking, Security and Risk/Compliance groups.
- Orchestrate response to incidents across disparate tools to move from detection to response faster and with less manual coordination.
- Combine threat detection with access protection to address insider threat and align with a program like Zero Trust.
- Address the number one threat vector with phishing training, multi-factor authentication, advanced spam filtering and DMARC to defend against Business Email Compromise.

Supporting resources
Read the report: Cisco 2019 CISO Benchmark Study
Follow us @Cisco

About Cisco
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.

View original content to download multimedia:http://www.prnewswire.com/news-releases/caution-security-startups-investors-and-standalone-solutionscisco-2019-ciso-benchmark-study-reports-increased-vendor-consolidation-300803837.html

SOURCE Cisco