State of Security 2022 Report Reveals Increase in Cyberattacks While Security Talent Remains Scarce

April 12, 2022

Global Research Shows Nearly Two-Thirds of Organizations Have Seen an Uptick in Cyberattacks and Roughly Half Experienced a Breach

SAN FRANCISCO--(BUSINESS WIRE)--Apr. 12, 2022-- Splunk Inc. (NASDAQ: SPLK), the data platform leader for security and observability, in collaboration with Enterprise Strategy Group, today released the State of Security 2022, an annual global research report that examines the security issues facing the modern enterprise. More than 1,200 security leaders participated in the survey, revealing they've seen an increase in cyberattacks while their teams are facing widening talent gaps.

According to the report, **65%** of respondents say they have seen an increase in attempted cyberattacks. In addition, many have been directly impacted by data breaches and costly ransomware attacks, which have left security teams exhausted:

- Nearly half (**49%**) of organizations say they have suffered a data breach over the past two years, an increase from 39% a year earlier.
- **79%** of respondents say they've encountered ransomware attacks, and **35%** admit that one or more of those attacks led them to lose access to data and systems.
- **59%** of security teams say they had to devote significant time and resources to remediation, an increase from 42% a year ago.
- **54%** of respondents report that their business-critical applications have suffered from unplanned outages related to cybersecurity incidents on at least a monthly basis, with a median of 12 outages per year.
    - The median time to recover from unplanned downtime tied to cybersecurity incidents is **14 hours**. Respondents estimated the cost of this downtime averaged about **$200,000 per hour.**
- **64%** of security professionals have stated that it's challenging to keep up with new security requirements, up from 49% a year ago.

"This survey has revealed that organizations are deeply concerned about supply chain attacks, especially after the SolarWinds hacks of 2020 and the Log4Shell incident in late 2021," said Ryan Kovar, Distinguished Security Strategist, Splunk. "Ninety percent of organizations reported that they have increased their focus on third-party risk assessments as a result of those high-profile attacks. In my 20 years in IT security, I've never seen software supply chain threats given this level of visibility. Unfortunately, this will only increase the already intense pressure security teams face."

As cybercriminals become more persistent and workloads increase, many organizations have been impacted by the Great Resignation and the additional security challenges of remote work. These factors have exacerbated the already ongoing talent shortage within the cybersecurity industry:

- **76%** of respondents say their team members have been forced to take on responsibilities they are not ready for, and **70%** say that the resulting increase in their workload has led them to consider looking for a new role.
    - **85%** of respondents say it has gotten harder to recruit and retain talent over the past 12 months.
- **53%** of respondents say they can't hire enough staff and **58%** cite an inability to find talent with the right skills.
    - **68%** of respondents report that talent shortages directly led to the failure of one or more projects/initiatives.
- **73%** of respondents say that workers have resigned, citing burnout.

Organizations from around the world face similar security challenges, but many struggle to secure proper investment into their cybersecurity programs and face cybersecurity skills shortages:

- Respondents in Canada report that their organizations are increasing their investment in cybersecurity at a slower rate than their counterparts globally. While **37%** of respondents say that their organization will increase investments significantly in the next 12-24 months, 52% of their peers in other countries say the same.
- Over half (**53%**) of German organizations reported that the struggle to recruit and retain security talent caused multiple project delays in the past 12 months, compared to 43% across other countries.
- Cybersecurity skills shortages appear to be particularly challenging in Singapore, with **44%** of respondents reporting challenges related to both hiring and retention, versus 22% of the peers globally reporting this to be the case.

"Our latest State of Security report has revealed the challenges security professionals face, but there are steps we can take to alleviate these issues," said Jane Wong, Vice President of Security Products, Splunk. "One positive sign is that over two-thirds (67%) of organizations are actively investing in technologies designed for advanced analytics and security operations automation. Automation is critical to help reduce the time it takes to respond to attacks, and these technologies should focus on assisting our human analysts, not replacing them. This can mean fewer tools, not more. For example, a platform approach can make it easier for security teams to take action on complex threats, while the basic stuff is remediated at machine speed. The result should be less sense of being overwhelmed — and less analyst burnout, but also reduced dwell time if the organization has been breached."

For more insights and recommendations from the State of Security 2022, please visit: www.splunk.com/en_us/campaigns/state-of-security.html

Methodology

The global survey was conducted from mid-January through mid-February 2022 and in partnership with the Enterprise Strategy Group. The 1,227 respondents, IT and security leaders and practitioners who spend more than half their time on security issues, were drawn from eleven regions: Australia, Canada, France, Germany, India, Japan, the Netherlands, New Zealand, Singapore, the United Kingdom and the United States.

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) helps organizations around the world turn data into doing. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale.

View source version on businesswire.com: https://www.businesswire.com/news/home/20220412005412/en/

Media Contact
Emil Hanscom
Splunk Inc.
press@splunk.com

Investor Contact
Ken Tinsley
Splunk Inc.
ir@splunk.com

Source: Splunk Inc.