



NEWS RELEASE

# Cybersecurity resilience emerges as top priority as 62 percent of companies say security incidents impacted business operations

2022-12-06

## News Summary:

- Security resilience is a high priority for 96 percent of executives, and rightfully so, as 62 percent of respondents say their organization experienced a recent security incident
- Executive support and cultivating a security culture were two of the top three success factors for achieving resilience
- Adoption of zero trust, secure access service edge, and extended detection and response technologies resulted in significant increases in resilient outcomes

MELBOURNE, Australia, Dec. 6, 2022 /PRNewswire/ -- CISCO LIVE -- Cybersecurity resilience is a top priority for companies as they look to defend against a rapidly evolving threat landscape, according to the latest edition of Cisco's annual Security Outcomes Report launched today.

Titled, *Security Outcomes Report, Volume 3: Achieving Security Resilience*, the study identifies the top seven success factors that boost enterprise security resilience, with a particular focus on cultural, environmental, and solution-based factors that businesses leverage to achieve security. The findings are based on survey responses from over 4,700 participants across 26 countries.

Resilience has emerged as a top priority as a staggering 62 percent of organizations surveyed said they had experienced a security event that impacted business in the past two years. The leading types of incidents were network or data breaches (51.5 percent), network or system outages (51.1 percent), ransomware events (46.7 percent) and distributed denial of service attacks (46.4 percent).

These incidents resulted in severe repercussions for the companies that experienced them, along with the ecosystem of organizations they do business with. The leading impacts cited include IT and communications interruption (62.6 percent), supply chain disruption (43 percent), impaired internal

operations (41.4 percent) and lasting brand damage (39.7 percent).

With stakes this high, it is no surprise that 96 percent of executives surveyed for the report said that security resilience is high priority for them. The findings further highlight that the main objectives of security resilience for security leaders and their teams are to prevent incidents, and mitigate losses when they occur.

"Technology is transforming businesses at a scale and speed never seen before. While this is creating new opportunities, it also brings with it challenges, especially on the security front. To be able to tackle these effectively, companies need the ability to anticipate, identify, and withstand cyber threats, and if breached be able to rapidly recover from one. That is what building resilience is all about," said Helen Patton, CISO, Cisco Security Business Group.

"Security, after all, is a risk business. As companies don't secure everything, everywhere, security resilience allows them to focus their security resources on the pieces of the business that add the most value to an organization, and ensure that value is protected," she added.

### **Seven Success Factors of Security Resilience**

This year's report has developed a methodology to generate a security resilience score for the organizations surveyed, and identified seven data-backed success factors. Organizations that had these factors present were among the top 90th percentile of resilient businesses. Conversely, those lacking them placed in the bottom 10th percentile of performers.

The findings of the study underline the fact that security is a human endeavor as leadership, company culture and resourcing have an oversized impact on resilience:

- Organizations that report poor security support from the C-suite scored 39 percent lower than those with strong executive support.
- Businesses that report an excellent security culture scored 46 percent higher on average than those without.
- Companies that maintain extra internal staffing and resources to respond to incidents resulted in a 15 percent boost in resilient outcomes.

In addition, businesses need to take care to reduce complexity when transitioning from on-premise to fully cloud-based environments:

- Companies whose technology infrastructures are either mostly on-premise or mostly cloud-based had the highest, and nearly identical, security resilience scores. However, businesses that are in the initial stages of transitioning from an on-premise to a hybrid cloud environment saw scores drop between 8.5 and 14 percent depending on how difficult the hybrid environments were to manage.

Finally, adopting and maturing advanced security solutions has significant impacts to resilient outcomes:

- Companies that reported implementing a mature Zero Trust model saw a 30 percent increase in resilience score compared to those that had none.
- Advanced extended detection and response capabilities correlated to an incredible 45 percent increase for organizations over those that report having no detection and response solutions.
- Converging networking and security into a mature, cloud-delivered secure access services edge boosted security resilience scores by 27 percent.

"The Security Outcomes Reports are a study into what works and what doesn't in cybersecurity. The ultimate goal is to cut through the noise in the market by identifying practices that lead to more secure outcomes for defenders," said Jeetu Patel, executive vice president and general manager of security and collaboration at Cisco. "This year we focused on identifying the key factors that elevate the security resilience of a business to among the very best in the industry."

#### **Additional Resources:**

- Report: [Security Outcomes Report, Volume 3: Achieving Security Resilience](#)
- Blog: [Cracking the Code to Security Resilience: Lessons from the Latest Cisco Security Outcomes Report](#)

#### **About Cisco**

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more on [The Newsroom](#) and follow us on Twitter at [@Cisco](#).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

View original content to download multimedia:<https://www.prnewswire.com/news-releases/cybersecurity-resilience-emerges-as-top-priority-as-62-percent-of-companies-say-security-incidents-impacted-business-operations-301696237.html>

SOURCE Cisco Systems, Inc.