censys

EXECUTIVE SUMMARY

The 2023 State of Security Leadership

Exploring the Struggles of CISOs in a Shifting Digital Terrain

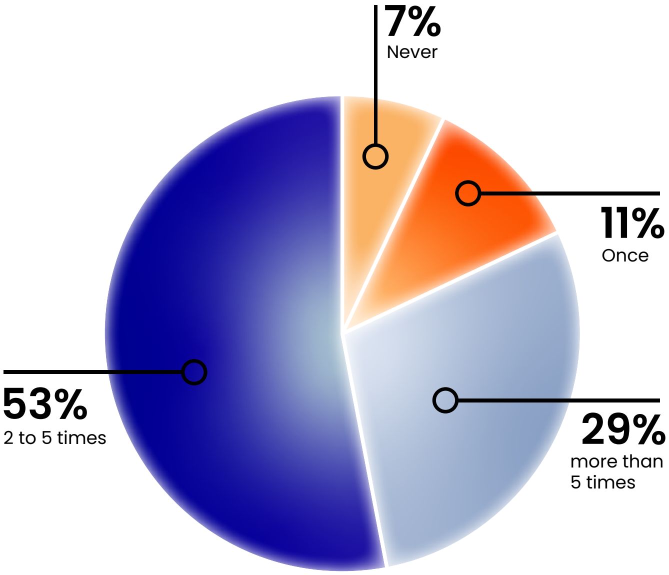
Censys conducted a study utilizing a blind quantitative survey to explore 208 total senior cybersecurity leaders' perspectives on strategic issues – from the current threat environment to geopolitical influence to personnel burnout, and more.

The job of the CISO has never been more challenging. Between the steady increase in ransomware attacks, the rise of geopolitical tensions and nation-state sponsored espionage, and the acceleration of trends like cloud migration, there is a LOT on the CISO's plate.

With so many challenging headwinds, how do CISOs hold it together to protect both their assets and their teams' wellbeing at the same time?

Key Findings

The threat outlook is not improving. All of our survey respondents reported that the cyber threat landscape is worse than the previous year. In fact, almost all respondents experienced at least one cyberattack and over half experienced between two and five. There was increased awareness of the amount and sophistication of attacks, especially attributed to conversations with their peers. Almost none said that a decrease in their own security budget contributed to this perception. It seems to be common knowledge and discourse in the industry.

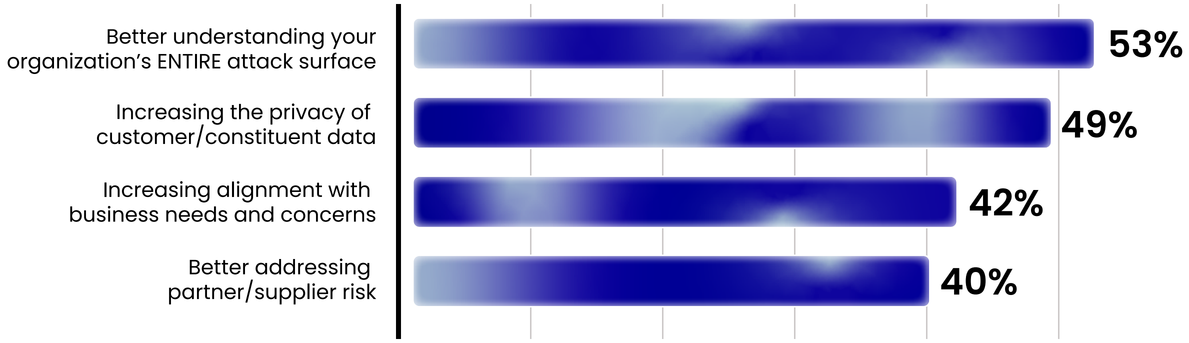


In the past 12 months, how many times was your organization affected by a cyberattack that caused material damage?

Geopolitics matter. Fifty-eight percent took defensive actions resulting from increased global tensions. With the war in Ukraine, today's divisive political landscape, and the ubiquity of globally distributed devices, nation-state actors are quickly taking advantage of this evolving paradigm. Additionally, the White House recently released their Cyber Security strategy, which stresses the importance of taking more vigilant action across both the public and private sectors.

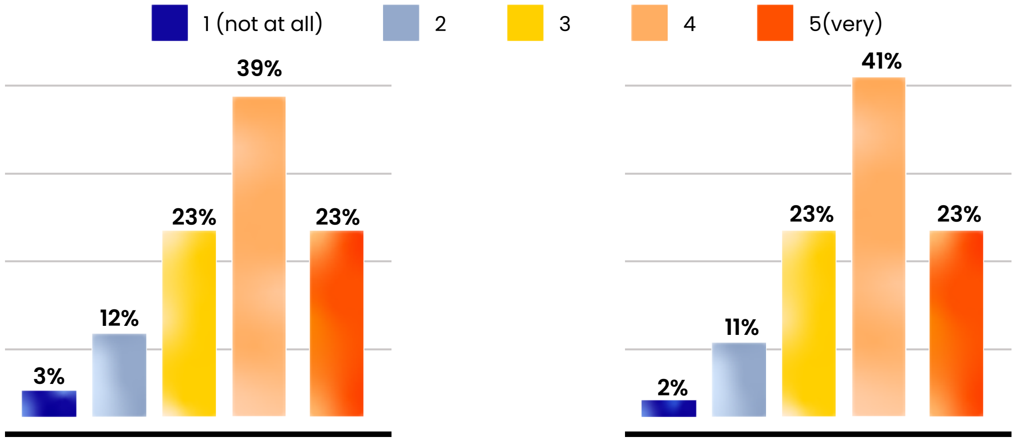
The breadth of connected assets is largely unknown. Over half of respondents said better understanding their entire attack surface is their top priority for the next twelve months. Most respondents currently have poor visibility into the range of digital assets connecting to their network—28% discover connected assets manually, and only 22% use an automated tool. Clearly, organizations still have a long way to go. And, even though it is well known that people are the weakest link in cyber risks, security leaders' efforts to control connected personal assets and workers' online behaviors aren't as strict as they likely should be.

Which of the following reflect your top priorities for improving your organization's cybersecurity over the next 12 months?



Security teams may be close to hitting the wall. Respondents indicated significant concerns about the talent shortage and the toll being taken on incumbent staff. With 65% citing the lack of qualified resources to fill their needs as their highest personnel worry, it is not surprising that over 60% of security leaders are reporting high levels of mental and physical burnout.

On a scale of 1 (lowest) to 5 (highest), please rate your level of concern regarding the following cybersecurity personnel issues:



Mental/physical burnout of you personally

Insufficient qualified resources to meet the cybersecurity requirements of your organization

censys

Censys can help! To get your hands on the FULL report, including our recommendations for effectively dealing with all of these challenges, visit censys.io/the-2023-state-of-security-leadership.

WEBSITE
www.censys.io

E-MAIL
hello@censys.io