Fastly Research Reveals 93% of Organizations Working to Reduce CISO Liability Risk

March 4, 2025

Increasing CISO involvement in strategic decisions at the board level and improving legal support for cybersecurity staff among the corporate policy changes

SAN FRANCISCO--(BUSINESS WIRE)-- Following a year that thrust Chief Information Security Officer (CISO) accountability into the spotlight, research from Fastly, Inc. (NYSE: FSLY), a leading global edge cloud platform provider, reveals that 93% of organizations made policy changes over the preceding 12 months to address concerns about increased personal liability for CISOs. This includes two in five organizations (41%) increasing CISO participation in strategic decisions at the board level.

In late 2023, newly adopted regulations such as the SEC rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies as well as other headlines have put an increased focus on corporate accountability for data breaches, raising an increased concern of CISO liability. To reduce this risk, 38% of Fastly research respondents have promised “increased scrutiny of security disclosure documentation from supervisory agencies” while 38% have improved legal support for cybersecurity staff, including liability insurance, and corporations have allocated more resources to security in the past year. While these steps are a positive development, Marshall Erwin, CISO at Fastly, questions whether these changes go far enough to protect organizations and their cybersecurity personnel.

“It’s encouraging to see the vast majority of companies making changes to liability disclosure given the inevitability of another worldwide outage that will put CISO accountability back into the spotlight. However, while investing in legal protection is an important step, this change is often more about shielding organizations from legal risk rather than fostering meaningful accountability to drive better security practices,” says **Fastly CISO, Marshall Erwin.** *“Proper accountability requires moving beyond liability insurance and disclosure edits. For meaningful change, we need to view accountability as a positive force to incentivize better security. For that, we need better, clearer standards from regulators and enforcers that distinguish between unavoidable incidents and avoidable ones resulting from truly deficient security practices.”*

Shared responsibility, not a single point of failure

Fastly’s research also found that nearly half (46%) of organizations are unclear about who holds ultimate responsibility for

cybersecurity incidents whilst only 36% have clearly delineated roles and responsibilities within their teams. The research points to a significant gap in how organizations internalize responsibility and translate regulatory guidance into meaningful improvements to security postures.

Marshall Erwin added, " *CISOs do not make the final call on every decision. When it comes to security risks, the question a board should be asking is, 'Are we aligning the budget to address the risks the CISO has communicated to us?' This is where accountability should start - at the senior leadership level, with clear communication and alignment of resources.* "

This responsibility doesn't just fall on one person - it requires clear communication at every level of the organisation to understand how and why cybersecurity risks should be mitigated and how efforts should be aligned to reduce exposure.

Creating better standards

The report underscores the need for the industry to prepare for the next high-profile incident with stronger frameworks for accountability that incentivise meaningful actions, rather than just compliance measures. As regulatory standards continue to evolve, organizations should recognize that CISO liability is not a threat but an opportunity to solidify security postures and drive long-term change across organisations.

About the research

This research surveyed 1,800 key IT decision makers with an influence in cybersecurity, in large organizations spanning multiple industries across North, Central and South America, Europe, Asia-Pacific and Japan. The interviews were conducted online by Sapio Research in September 2024 using an email invitation and an online survey.

To access the full set of data and understand how businesses are consolidating tools and changing their spending habits in the wake of high-profile cybersecurity incidents, visit here.

About Fastly, Inc.

Fastly's powerful and programmable edge cloud platform helps the world's top brands deliver online experiences that are fast, safe, and engaging through edge compute, delivery, security, and observability offerings that improve site performance, enhance security, and empower innovation at global scale. Compared to other providers, Fastly's powerful, high-performance, and modern platform architecture empowers developers to deliver secure websites and apps with rapid time-to-market and demonstrated, industry-leading cost savings. Organizations around the world trust Fastly to help them upgrade the internet experience, including Reddit, Neiman Marcus, Universal Music Group, and SeatGeek. Learn more about Fastly at https://www.fastly.com, and follow us @fastly.

Source: Fastly, Inc.

Media Contact
Alex Klepel
press@fastly.com

Investor Contact
Vernon Essi, Jr.
ir@fastly.com

Source: Fastly, Inc.