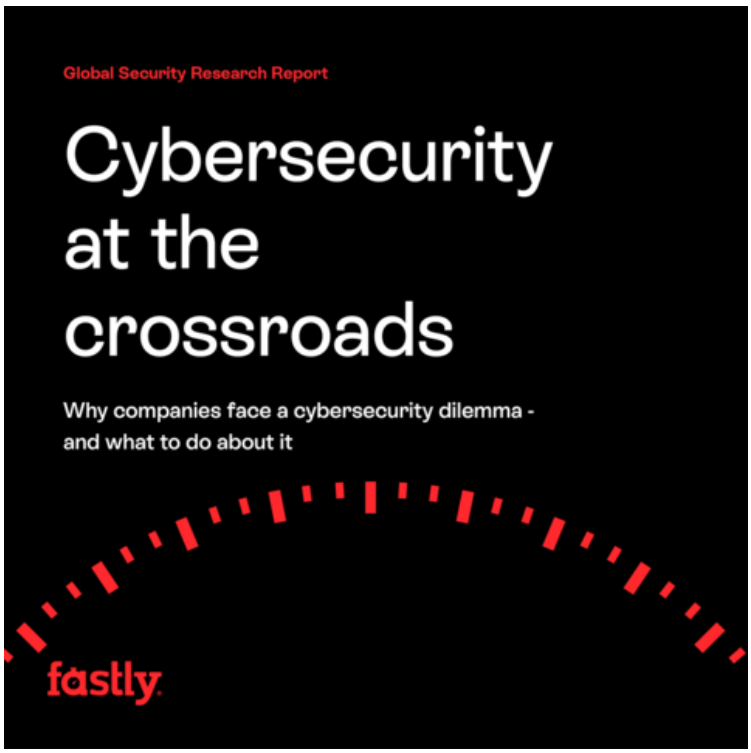
# Long Road to Recovery: Fastly Research Reveals Businesses Taking 25% Longer to Recover From Cybersecurity Incidents Than Expected

November 19, 2024

*Organizations are reassessing their cybersecurity budget allocations after taking 7.3 months to recover from incidents in 2024 - over a month longer than expected*

SAN FRANCISCO--(BUSINESS WIRE)-- Fastly, Inc. (NYSE: FSLY), a leader in global edge cloud platforms, has launched its latest annual Global Security Research Report, revealing a rise in the time it takes businesses to recover from cyber incidents. In 2024, businesses reported taking an average of 7.3 months to recover from cybersecurity breaches - 25% longer than expected and over a month past the anticipated timeline of 5.9 months.




Recovery times were even worse for companies that planned on cutting back cybersecurity spending. They faced an average of 68 incidents each – 70% above the average – and their recovery times stretched to 10.9 months, more than five months longer than those maintaining or increasing their budgets.

With attacks becoming more prevalent and taking longer to recover from, not surprisingly, the report found that 87% of businesses do plan to increase investment in security tools over the next 12 months, an 11% year-on-year rise. However, despite the additional spending, half of the surveyed cybersecurity decision makers (50%) feel that an increasingly sophisticated threat landscape has still left them unprepared to deal with future attacks.

**Marshall Erwin, CISO at Fastly, commented on the findings,** *"Full recovery from breaches is not getting any faster. The revenue, reputation and time lost damages business relationships permanently and drains resources from other areas of the business. With attacks not diminishing and the possibility of further high-profile slip-ups always present, it's crucial that any changes businesses are now making to cybersecurity strategies fit within a holistic plan and aren't knee-jerk reactions."*

Recent global IT outages have also been a wake up call for security professionals with many now scrutinizing their vendor choices and the value of cybersecurity investments more closely. In 2024, 40% of businesses expressed concerns about the reliability and software quality across their security stack and nearly one third (29%) considered changing vendors (a figure that rises to 37% in the US). In addition, the vast majority of businesses (86%) have changed their approach to testing and rolling out updates in response to major reliability incidents.

When it comes to software security, we found that organizations are also re-evaluating how security integrates across their operations. Increasingly, key stakeholders outside traditional security teams, including Platform Engineering teams, are having a say in which app security solutions are being adopted, with one in five (20%) saying their organization's priority was to adopt a platform engineering approach to software security. This is also reflected in a change in culpability, with Platform Engineering teams held responsible for 8% of cybersecurity incidents, only slightly down from CISOs at 14% and CIOs at 12%.

**Marshall Erwin added,** *"Cybersecurity spending is under the microscope as businesses continue to feel unprepared dealing with an evolving threat landscape. We are seeing a shift towards a shared responsibility for security across organizations, with increased focus on embedding security measures throughout all projects. Companies that bake in security and establish strong partnerships with security organizations early in a product development process are in a better position to deal with emerging threats and recover more quickly from attacks."*

**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 report 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.