NEWS RELEASE

The $600 Billion Wake-up Call: New Splunk Research Reveals Downtime is a Systemic Business Crisis

2026-05-19

- ***$600 Billion Annual Impact:*** *Aggregate downtime costs for the Global 2000 have soared 50% in two years.*
- ***$15,000 Per Minute:*** *The average cost of downtime for organizations, highlighting the immediate financial impact of service disruptions.*
- ***3.4% Stock Price Drop:*** *The average decline in shareholder value following a single downtime incident.*

SAN JOSE, Calif., May 19, 2026 /PRNewswire/ -- Cisco today announced the release of Splunk's latest research, *The Hidden Costs of Downtime,* revealing the aggregate cost of unplanned downtime for Global 2000 companies has surged to $600 billion annually – a 50% increase in just two years.

In partnership with Oxford Economics, the Splunk study shows that the financial toll of an outage is immediate, severe, and potentially long-lasting. Downtime has become a systemic business crisis that threatens revenue, brand equity and shareholder value, costing an organization $95 million in lost revenue annually. This is nearly twice the level seen in 2024.

"Downtime is inevitable; prolonged disruption is not," said Kamal Hathi, SVP and GM, Splunk, a Cisco company. "The most resilient organizations are not the ones with the most tools or the biggest vision for AI. They are the ones that align technology with business outcomes, empower people with context, and design systems that bend, but do not break, under pressure."

The Business Impact of Downtime
Technology executives increasingly view the consequences of an outage as *more severe.* Publicly disclosing a data breach is now considered the most severe hidden cost, with 71% of technology executives rating it as *very* or *prohibitively disruptive*, up from 23% in 2024. Furthermore, downtime triggers a chain reaction of hidden costs, including:

- **Financial and Market Erosion:** The study found that the average cost of downtime has reached $15,000 per minute. In addition, organizations see an average 3.4% drop in stock price following a downtime event.
- **Customer Churn:** Eighty-one percent of technology leaders cite the loss of customers as a consequence of downtime, with 47% admitting customers are *often* or *very often* the first to detect service degradation or outages.
- **Escalating Ransomware Costs:** Ransomware payouts have nearly tripled since 2024, now reaching $40 million on average, making them one of the most significant direct financial burdens.
- **Regulatory Exposure:** Regulatory fines have reached an average of $51 million per organization, with 57% of technology executives now viewing these penalties as *very or prohibitively disruptive*.
- **Operational Drag:** A staggering 89% of tech leaders cite the need for large numbers of personnel to fix issues. Nearly all (90%) tech leaders report increased demand for customer support with 76% of finance and 74% of marketing executives feeling the pressure as well.
- **Brand Recovery:** Nearly 20% of marketing professionals report that it takes an entire quarter to recover brand health following remediation.

The Intersection of Security and Downtime
About one-third (36%) of security leaders admit that downtime is *often* or *very often* misclassified as an IT issue, which can give attackers a critical head start. A lack of shared context complicates resolution, as only 38% of technology executives report consistently identifying the root cause of a downtime incident. The perceived frequency of cybersecurity-related downtime caused by SaaS and other third-party application issues has nearly tripled since 2024, with 56% of security leaders now experiencing these issues *often* or *very often*. Maintaining basic cyber hygiene and modernizing legacy infrastructure to replace outdated, unpatchable technology remain foundational to preventing unplanned downtime.

The Evolving Role of AI in Resilience
Organizations are increasingly turning to AI to enhance incident triage and root cause analysis, with a median annual spend of $24.5 million on AI tools that prevent and respond to downtime. As these technologies mature, the industry is shifting toward a model of human-to-agent collaboration, where AI serves the expert rather than replacing human oversight. This approach relies on machine data, the logs, metrics, and traces that allow teams to monitor AI actions, detect issues early, and correct course before minor errors escalate into full-scale outages.

The data reveals that organizations identified as "AI Workflow and Triage Experts," are significantly better equipped to avoid the most damaging outcomes of downtime:

- **Higher Resilience for AI Experts:** 74% of these experts avoided the need to publicly disclose a data breach last year, compared to just 54% of non-experts.
- **Customer Retention:** These expert organizations are nearly three times more likely to report that they have never lost customers due to downtime (42% versus 15% for non-experts).

Despite the clear benefits, the transition to autonomous systems is not without challenges. While 56% of users report that AI has reduced their overall risk, every technology leader surveyed admitted their organization has experienced some form of AI-related downtime. Sixty-eight percent of technology leaders express concern their AI agents will behave unpredictably, underscoring the need for robust governance and human-in-the-loop oversight that defines true digital resilience.

Building True Resilience
Technology executives increasingly recognize the need to visualize the entire digital dependency chain. In fact, among organizations with the lowest downtime costs, a massive 98% confirm that end-to-end visibility is *very* or *extremely important* for reducing incidents. Nevertheless, complete visibility remains rare across IT domains, prompting organizations to shift their investment strategies toward more

proactive, data-driven foundations:

- **Prioritizing Observability:** About three-fourths of ITOps and engineering leaders identify end-to-end observability as their top investment priority to improve infrastructure resilience, taking precedence over traditional hardware or data center upgrades.
- **Automating to Reduce Human Error:** Sixty-six percent of ITOps and engineering leaders are prioritizing investments in automation to mitigate the risks of human error, which remains the leading cause of downtime across the technology stack.
- **Targeting AI Investments:** Organizations are focusing their AI budgets on high-impact areas, with 85% of technology leaders prioritizing AI-driven security automation and 65% investing in AI-powered observability to gain deeper, real-time insights into their digital ecosystems.

For further details on methodology and findings of *The Hidden Costs of Downtime* report, please visit the Splunk website.

Methodology
Oxford Economics fielded a hybrid survey using CATI (Computer Assisted Telephonic Interviewing) and online methods. The fieldwork captured responses from 2,000 executives from Global 2000 companies. Businesses from 20 countries are represented from APAC, EMEA, North America, and LATAM. Respondents hail from nine industry groups: financial services, retail and consumer goods, public sector, manufacturing, energy and utilities, healthcare and life sciences, information services and technology, transportation and logistics, and communications and media. Respondents come from technology (including security, IT, and engineering titles), finance (including Chief Financial Officers), and marketing functions (including Chief Marketing Officers).

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide technology leader that is revolutionizing the way organizations connect and protect in the AI era. For more than 40 years, Cisco has securely connected the world. With its industry leading AI-powered solutions and services, Cisco enables its customers, partners and communities to unlock innovation, enhance productivity and strengthen digital resilience. With purpose at its core, Cisco remains committed to creating a more connected and inclusive future for all. Discover more on The Newsroom and follow us on X at @Cisco.

About Splunk LLC
Splunk, a Cisco company, helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation.

View original content to download multimedia:https://www.prnewswire.com/news-releases/the-600-

billion-wake-up-call-new-splunk-research-reveals-downtime-is-a-systemic-business-crisis-302774919.html

SOURCE Cisco Systems, Inc.