



The Hidden Costs of Downtime in Manufacturing

We surveyed executives across the Global 2000 to explore the depths of downtime: what it costs, what causes it, and what leading organizations are doing right. Here, we highlight findings from respondents in the manufacturing industry.

\$255 million

The annual cost of downtime for manufacturing organizations is \$255 million annually.

Manufacturing experiences more cybersecurity-related downtime than most industries. So, it comes as no surprise that manufacturing has the second-highest cost of downtime of any industry, with revenue loss (\$58M) accounting for nearly a quarter of all downtime-related expenses.

But other direct costs add up, too. Respondents cite regulatory fines (\$40M) and penalties from missed SLAs (\$24M) as other top cost drivers.

Beneath the surface are hidden costs and industry interdependencies. When manufacturers are down, it upends every aspect of the supply chain and downstream organizations, such as retailers and logistics companies.

Downtime can come from anywhere

Downtime isn't just an ITOps or engineering issue. It's a security one as well. Understanding the most common culprits can help companies manage incident response and possibly prevent lightning from striking twice.

The Global 2000 confirmed downtime's dual origins: 56% come from security incidents while 44% stem from application or infrastructure issues.

Cybersecurity-related human error is "often" or "very often" the offender, according to 60% of manufacturing organizations. Other top cybersecurity-related downtime causes include:



Cybersecurity-related human error results in the most downtime and takes the longest to detect and remediate — with manufacturers fixing issues more slowly than most other industries on average.

19 hours

Mean time to detect (MTTD)

87 hours

Mean time to recover (MTTR)



Tackling downtime with smart technology investments

Manufacturing organizations spend a combined \$59.5M on cybersecurity tools (\$33.2M) and observability tools (\$26.3M) annually. Considering the industry's high attack volume and high cost of downtime, manufacturing cybersecurity spending ranks second highest across all industries.

No other technology has made as much of a splash recently as generative AI: 68% use discrete generative AI tools (e.g., ChatGPT) to address downtime.

Meanwhile, 49% use generative AI features embedded into existing tools, such as AI assistants that help write queries and troubleshoot.

Manufacturing organizations' toughest obstacles to managing downtime

Percentage of respondents who experienced	Challenge
76%	Data sprawl
57%	Too many false positives/alert fatigue
48%	Lack of understanding of system interdependencies
46%	Tools are too expensive

Manufacturing organizations can champion a more resilient business

Learn more about the hidden costs of downtime and how Splunk can help your organization steer clear of its costly consequences.

[Get the full report >](#)

[Manufacturing overview >](#)



Cost of downtime checklist: A guide for tackling downtime in manufacturing

Unplanned downtime inflicts real financial damage on manufacturers. But the fallout doesn't end there. When manufacturers are down, it upends every aspect of the supply chain and downstream organizations, like retailers and logistics companies. For manufacturers, it can be hard to know what actions to take to minimize downtime.

Here's a list of considerations to ensure you're taking the right steps for your organization.

Questions to ask	How do I compare?	How can I take action?
Does my organization have a plan for improving our downtime costs? Yes: ☐ No: ☐	\$255M is the average annual cost of downtime for manufacturers.	☐ Practice good corporate hygiene by instrumenting every OT device and app, following a runbook for outages, and identifying owning engineers. ☐ Perform regular exercises and hypothetical scenarios with your SecOps, ITOps, OT, and engineering teams. ☐ Consider adopting "chaos engineering," real drills that build a more resilient system.
Can my organization identify our top causes of cybersecurity-related downtime? Yes: ☐ No: ☐	60% say human error is the top cybersecurity-related downtime cause, with 38% citing malware attacks.	☐ Pursue root cause analysis during incident response to single out the underlying problem and point to a fix. ☐ Invest in observability tooling and integrate data from across your IT and OT environment into one centralized location to isolate root causes. ☐ Eliminate silos to access data across devices and tools and perform rigorous postmortems to avert repeat occurrences.
Does my organization use generative AI to help address downtime? Yes: ☐ No: ☐	49% currently use generative AI features embedded into existing tools to manage downtime.	☐ Opt for embedding generative AI features into existing tools — e.g., AI chat bots — to help address downtime and improve productivity. ☐ Keep in mind that inputting company intellectual property (IP) into any Large Language Model (LLM) comes with security risks — establish a clear data governance policy to safeguard your organization from data leakage.
Is my organization investing in visibility tools that help manage and prevent downtime? Yes: ☐ No: ☐	\$26.3M is spent on observability tools in manufacturing annually.	☐ Focus on data management and tool consolidation that leads to comprehensive visibility and cross-collaboration across SecOps, ITOps, and engineering. ☐ Prioritize solutions that address downtime's dual origins: cyberattacks and application or infrastructure issues. ☐ Share tools, data, and context to help teams collaborate, fix problems, and identify root causes when downtime occurs.
Does my organization have a plan to address the obstacles that slow response times? Yes: ☐ No: ☐	76% cite data sprawl and 57% name too many false positives and alert fatigue as top obstacles.	☐ Empower your SecOps, ITOps, OT, and engineering teams with a proactive and collaborative downtime prevention program by investing in AI- and ML-driven solutions. ☐ Deploy predictive analytics powered by AI as a force multiplier to help prevent issues from becoming five-alarm fires.

If you answered "no" to any of these questions, we're here to help. [Contact us](#) now to learn how you can minimize downtime and champion a more resilient business.

Learn how Splunk supports manufacturers on their path to digital resilience.