The Hidden Costs of Downtime

The $400B problem facing the Global 2000

splunk>

Disruption in business is inevitable. The most successful organizations today adapt to system stressors and bounce back quickly because they invest in a solid foundation of digital resilience. And yet, unplanned downtime continues to test that resilience and, in many cases, exacts a significant toll.

The true financial impact and nature of downtime are hard to pin down. Researchers often focus only on downtime caused by traditional IT issues, overlooking incidents brought on by cybersecurity failures, while also leaving secondary economic ramifications out of the equation. We weren't satisfied with an incomplete picture.

In partnership with Oxford Economics, a global research institute, Splunk quantified the total cost of downtime for the Global 2000 to be $400 billion annually. These companies lose $200 million on average each year because their digital environments fail unexpectedly.

It turns out, there is also much more beneath the surface. We uncovered considerable hidden costs — like billion-dollar impacts to market cap — that may deal an even larger economic blow to companies. The data also confirmed what we've long suspected: Cybersecurity and infrastructure or application issues are both sources of downtime.

I'm pleased to share *The Hidden Costs of Downtime*, a first-of-its-kind report that examines the direct and historically overlooked costs of unplanned downtime, reveals its most common causes, and uncovers how the most resilient organizations predict and prevent its repercussions.

The findings are clear: The financial impact of downtime should have every board and every technology leader making digital resilience a priority. It's imperative that executives understand the effects of downtime on their organizations and take the necessary steps toward resilience across their entire digital footprint.

Gary Steele
President, Go-to-Market, Cisco
GM, Splunk

Exploring the depths of downtime

Every week, it seems the media treats us to headlines like "Multinational Telecommunications Company Suffers Global System Outage" and "Hospital Closes Temporarily From Cyberattack, Putting Patients and Medical Records at Risk." A CEO apology, social media firestorms, and tumbling stocks often accompany these stories.

Unplanned downtime[1] — any service degradation or outage of a business system — can be a frustrating inconvenience or even a life-threatening scenario for customers. For companies, downtime inflicts real financial damage in the form of regulatory fines, lost revenue, overtime wages, and much more.

It all adds up.

We surveyed 2,000 executives from the Global 2000[2] and, with the help of Oxford Economics, calculated the average cost of downtime at $400B per year. That works out to $200M per company, or roughly 9% of profits,[3] which is significant by any measure.

And those are just direct costs. Hidden costs can also make a sizable dent in the bottom line. We're talking about things like a dip in stock price. Delayed time-to-market that creates an opening for competitors to lure customers away. Tarnished brand reputation that erodes customer and investor trust. The list goes on.

It's not much of a leap to see that these and other hidden costs could easily amount to more than $200M annually for a single company. And we've found that organizations pay for these consequences long after systems recover — months, in fact.

We also explored the causes of downtime and discovered it just as often originates from cybersecurity issues as infrastructure or application problems. This suggests that successful mitigation strategies will consider both realms. The data revealed an upper echelon of companies that take that approach. They are more resilient than the majority of respondents, suffering less downtime and its consequences.

In this report, we explore the depths of downtime: what it costs, what causes it, and what leading organizations are doing right.

Let's dive in.

1 For the context of our survey, downtime was defined as any type of service degradation (such as latency/slowness), as well as service unavailability to end users of critical business systems.

2 "The Global 2000 ranks the largest companies in the world using four metrics: sales, profits, assets, and market value." (Forbes)

3 Figure derived from the 2023 Forbes Global 2000 collective $4.4T in profits.

Contents

3 Exploring the depths of downtime

4 There is more to downtime than meets the eye

9 Downtime can come from anywhere

13 Tackling downtime with smart technology investments

17 Resilience leaders know the ropes

22 Navigating downtime at your organization

24 Downtime looks different in every industry

25 The costs of downtime around the world

27 Methodology

There is more to downtime than meets the eye

“If you look at the cost of downtime, it’s a significant amount because there might be 15 senior technical people sitting around a table at x per hour, working out what’s the root cause. What are we going to do? How do we manage the collateral damage? How do we manage the customer? How do we manage the regulator?”

— Chris Russell Miller, Head of IT and Cyber Risk, BNP Paribas Personal Finance UK

Breaking down the direct costs of downtime

The economic effects of downtime aren't limited to a single department or cost category. To paint a fuller picture, we surveyed CFOs and CMOs who could speak to the broader brand and financial fallout of poor digital experiences, as well as security, ITOps, and engineering professionals. We asked respondents to quantify the cost of downtime across several dimensions, and it's clear that downtime is a business concern, not just a technical one.

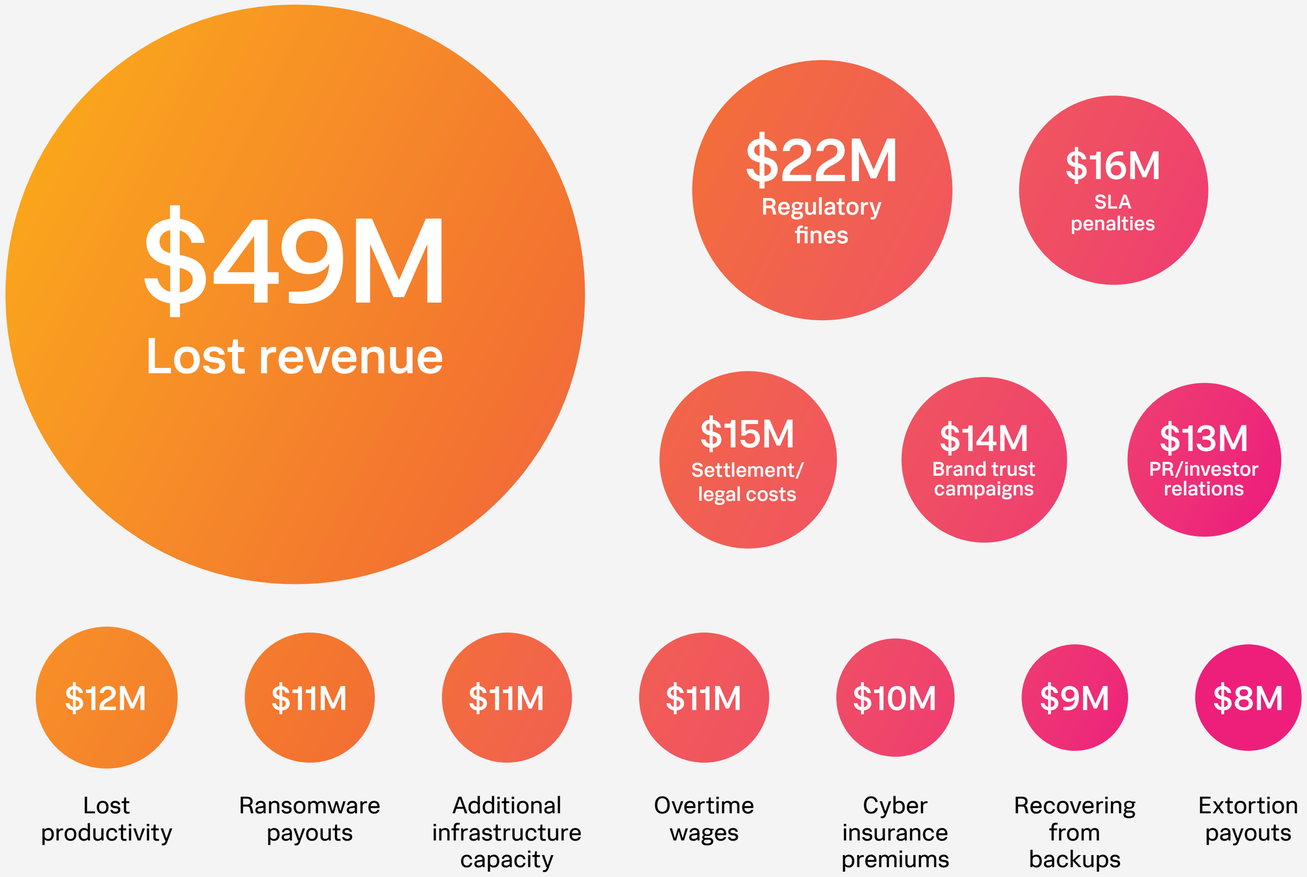
Based on survey responses, Oxford Economics calculated that downtime costs Global 2000 companies $400B annually. That's $200M per company per year, roughly 9% of profits. Every minute of downtime costs an average of $9,000 or $540,000 per hour.

What's driving this number? Let's break it down.

Lost revenue is number one on the list of direct costs at $49M annually. It's more than double the second-highest cost. Obviously, lost revenue stings. Sixty-one percent of all respondents call it "very" or "prohibitively" damaging, and according to CFOs we surveyed, it takes 75 days for revenue to recover.

The direct costs of downtime dent the bottom line

Lost revenue is by far the biggest financial impact, but other direct costs add up, too.

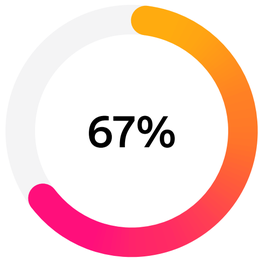


Dollar amounts are rounded to the nearest whole number.

Regulatory fines, which average $22M per year, are next on the list of direct costs. Seventy-nine percent of technology executives surveyed confirmed their organization's country or region places strict regulations on downtime — such as the Digital Operational Resilience Act (DORA) for the financial sector in the EU. This regulatory trend makes resilience essential to maintaining compliance and avoiding fines that can hurt the bottom line.

How else does downtime disrupt the balance sheet? According to CMOs, companies spend, on average, $14M to repair their reputations by conducting brand trust campaigns and another $13M increasing programs for public, investor, and government relations. CMOs also acknowledge downtime's influence on their jobs: 72% say minimizing downtime is "important" or "very important" to their role.

Cyberattacks also drain budgets. Sixty-seven percent of CFO respondents say that when their organization suffers a ransomware attack, they usually advise their CEO and board of directors to pay up, either directly to the perpetrator, through insurance, a third party, or, most commonly, some combination of the three. Ransomware payouts ($11M) and extortion payouts from ransomware attacks ($8M) total $19M annually.

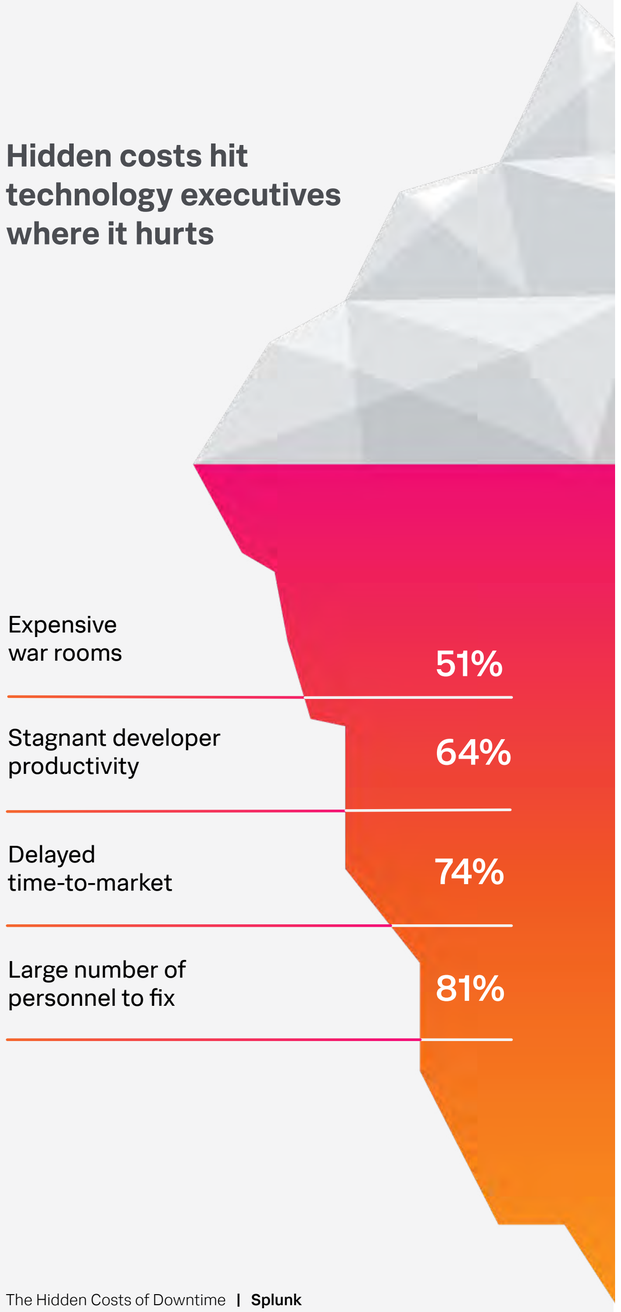


Of CFOs say they advise their CEO and board to pay the ransom

> **Whatever margin you're getting from your customers, you have to deduct the cost of downtime from those margins. You lose revenue, and if it continues to happen, you lose your reputation and bear permanent loss of business.**

— Mauli Tikkiwal, IT Director and Board Member at a multinational manufacturing company

Hidden costs hit technology executives where it hurts



The hidden costs of downtime are hard to ignore

Relatively trickier to measure and less visible, the hidden costs of downtime are likely just as impactful as direct costs. Downtime creates a tidal wave of side effects that reach every corner of an organization. From security, ITOps, and engineering teams stuck in the maze of root cause analysis to CMOs forced to pivot marketing and communications to crisis management — and even CFOs watching stock prices plunge in the blink of an eye.

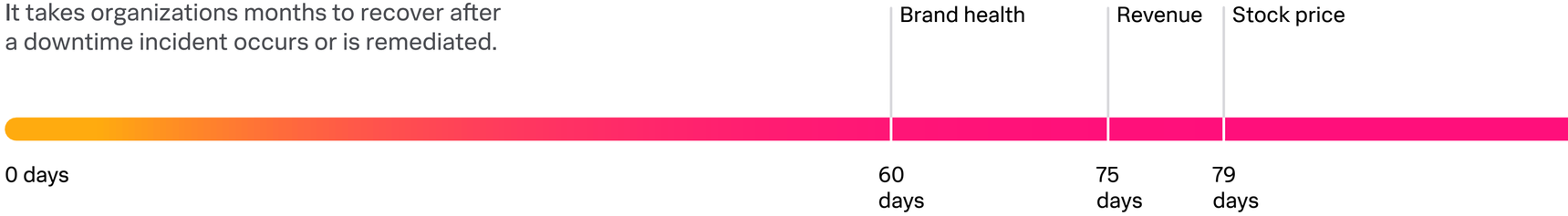
When downtime occurs, whole teams must shift from high-value work (like launching new digital products and experiences) to applying software patches and participating in postmortems. Practitioners know that during an incident, everyone gets called into a conference bridge, and no one is off the hook until the issue is resolved. Productivity plummets, innovation velocity and time-to-market slows, hurting competitive position and likely costing upwards of tens of millions in aggregate.

Respondents are also troubled by personal risks that can accompany downtime. Thirty-nine percent of technology respondents worry about being found personally liable for an incident, and another 38% fear that downtime might affect their performance review — or even lead to termination.

Perhaps the most significant hidden cost? Twenty-eight percent of all respondents say downtime diminishes shareholder value. Organizations can expect their stock price to drop between 1% and 9% after a single downtime event (2.5% on average) and to take an average of 79 days to recover. Ouch.

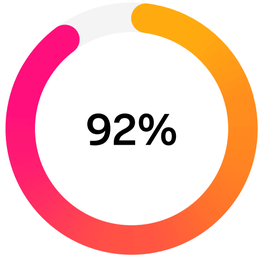
The long road to recovery

It takes organizations months to recover after a downtime incident occurs or is remediated.



Downtime sinks lifetime value

It's never a good look when your customer knows more about your digital experience than you. Yet, 41% of technology executives admit customers are "often" or "always" the first to detect downtime. It can ruin the customer experience, dilute customer loyalty, and damage public perception when an incident sparks a social media frenzy. In fact, 40% of CMOs reveal that downtime impacts average customer lifetime value (CLV), and another 40% say it damages reseller and/or partner relationships.



Of CMOs say downtime puts their marketing department at a competitive disadvantage

Twenty-nine percent of respondents say they've lost customers because of downtime, while another 44% claim that downtime damages their reputation. CMOs report that it takes an average of 60 days to recover brand health after remediating an incident. Downtime's influence on customer loyalty and reputation is too glaring to ignore, forcing CMOs to act swiftly or get caught in the riptide.

Of course, as with all systems outages, reputational damage, net promoter scores, and people posting on social media are the collateral damage of these types of incidents.

— Chris Russell Miller, Head of IT and Cyber Risk, BNP Paribas Personal Finance UK

The downstream effects of downtime on marketing

67%
Increased advertising for brand trust campaigns

67%
Pivoted teams to crisis management

65%
Generated national or international news at least once

62%
Lost marketing and sales productivity

61%
Diverted budget to crisis management

Downtime can come from anywhere

“Cybersecurity downtime is the most expensive way to understand downtime in general.”

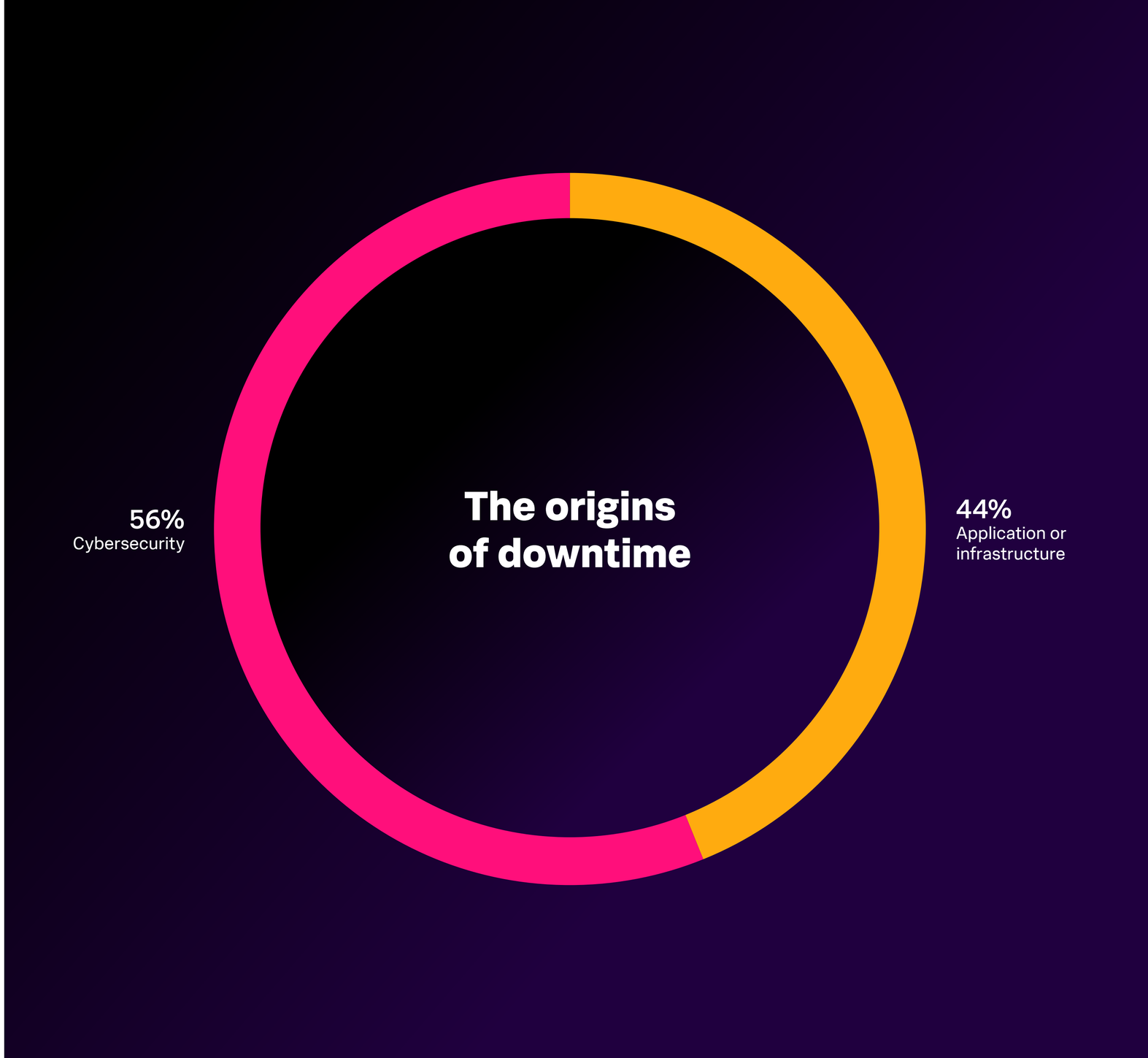
— Luca Panattoni, Head of IT and Digital Transformation, Carrefour

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. Our respondents confirmed downtime's dual origins: 56% spring from security incidents such as phishing attacks, while 44% stem from application or infrastructure issues like software failures. In both scenarios, human error is the number one offender and the toughest to detect and remediate.

While availability for most systems is at multiple 9s, downtime across hundreds — or perhaps thousands — of systems adds up. On average, a typical Global 2000 company sees 466 hours of cybersecurity-related downtime and 456 hours of application or infrastructure-related downtime.

Most of the time, cyberattacks happen because you are not keeping up with the evolving technologies and the threats it brings to your business.

— Mauli Tikkiwal, IT Director and Board Member at a multinational manufacturing company



Human error drives downtime

Human error — such as misconfiguring software or infrastructure — is the number one cause of downtime, with half of all respondents declaring it is “often” or “very often” to blame. Making mistakes like these can lead to performance errors that drag systems down or put a company’s security at risk.

Human error also takes the longest to detect and remediate. Seventeen to 18 hours tick by on average before organizations notice an incident. And it takes another 67-76 hours to recover from human error-related downtime and service degradation (such as latency). It’s not unusual for latency or slowness to affect systems for several days.

Security incidents: After human error, security respondents flag malware and phishing attacks as the most frequent causes of downtime. Meanwhile, security respondents say some of the rarest incidents take longer to detect and remediate. For instance, a “zero-day” exploit takes its name from leveraging a previously unknown system flaw to gain entry. Therefore, the detection and recovery times are likely extended because it’s difficult to pinpoint a root cause, and organizations often lack standard processes to address this unusual occurrence. Major downtime events that make headlines (utility company outages, hotel cyberattacks) are reminders that getting back online is no small feat.

ITOps and engineering incidents: Besides human error, software failure shoulders the most responsibility for downtime, as organizations adopt modern development and deployment practices that are more complex with added points of failure. Forty-nine percent of respondents say software failure was “often” or “very often” to blame for outages, and 34% point the finger at hardware failure. Remediating a software failure takes 16 hours on average. In our experience, organizations typically restore service much sooner than that, but we suspect respondents included fixing the root cause and conducting a thorough postmortem in their calculations.

The most common causes of downtime

1. Cybersecurity-related human error
2. ITOps-related human error[4]
3. Software failure
4. Malware attack
5. Hardware failure
6. Phishing attack
7. Third-party software outage

4 Infrastructure misconfigurations, capacity issues, and application code errors

We have downtime every day, sometimes multiple times a day — latency issues, performance degradation, or services being completely down.

— Poonam Khemwani, Executive Director, IT and Cloud Security Architecture, JPMorgan Chase

Rooting out the root cause

Sixty-three percent of technology respondents claim they always fix the root cause of a downtime incident, but that doesn't mean they can stop the same class of incidents from recurring. Isolating a problem within a complicated hybrid environment of cloud-based and legacy systems can be grueling. Fifty-four percent of tech executives admit they sometimes intentionally leave root causes of downtime unfixed — perhaps because they don't want to increase the technical debt of their legacy systems or they already plan to decommission the antiquated application responsible for the outage.

Finding and fixing root causes during postmortems is an industry best practice, but without the proper tooling, they can be difficult and time-consuming. Done correctly, postmortems make an entire infrastructure more robust and reliable. However, only 42% of technology executives say their organization always performs a postmortem. Sometimes, downtime is over so quickly or has such a small impact that it isn't worth investigating for many large enterprises.

It's always to our benefit to find the root cause so we can prevent it from happening again. Downtime is actually monitored right up to our CEO level.

— A VP of IT Architecture and Cybersecurity at a large U.S. telecommunications company

Tackling downtime with smart technology investments

“It’s about educating the business and finance communities on the implications of not prioritizing technology upgrades or investing in better technologies to keep up.”

— Mauli Tikkiwal, IT Director and Board Member at a multinational manufacturing company

Investing in resilience pays off

Naturally, companies go to great lengths to avoid a downtime disaster. Besides investing in best-in-class talent to keep their services up and running, on average, organizations spend a combined $43.3M annually on cybersecurity tools ($23.8M) and observability tools ($19.5M).

Even with substantial mitigation investments, companies hedge against worst-case scenarios. CFOs dole out an average of $34.8M annually on cybersecurity insurance and budget $13.4M for ransomware and data extortion payouts. However, that's not nearly enough: Companies actually spend $19M per year on payouts. Realistically, it may be necessary for CFOs to increase the budget.

So, are these costs worth it? According to our respondents — they are. The overwhelming majority of technology executives say their cybersecurity and observability tools are "helpful" or "extremely helpful" in addressing downtime. CFOs agree: at least 84% claim they get a solid ROI from security, ITOps, and engineering investments.

Knowing that downtime comes from cyberattacks as well as infrastructure and application issues, organizations should think holistically about their investments, prioritizing solutions that can address both causes. The vast majority of CFOs say protecting against all types of downtime is either "important" or "very important" in corporate funding strategy.

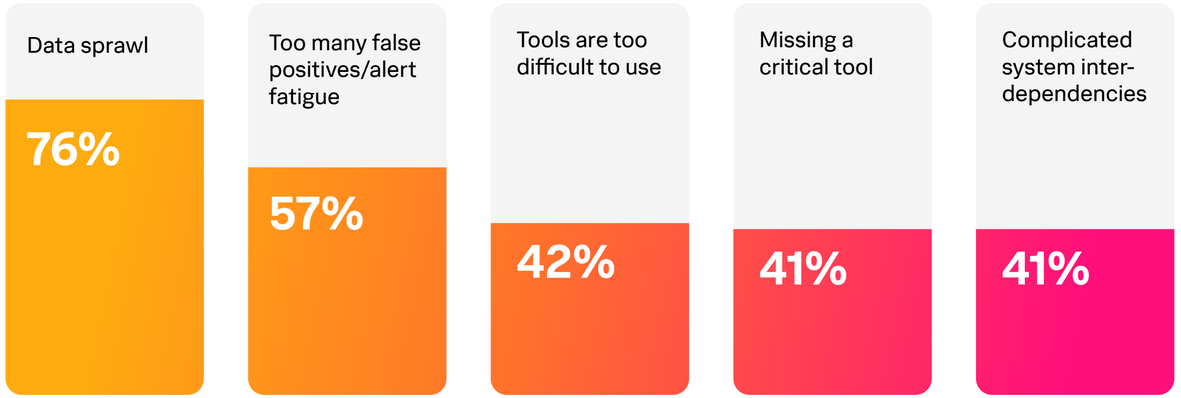
Despite significant tool investments, tackling downtime is still a formidable challenge.

Exploding data volumes, combined with data decentralization across tools and clouds, obscure visibility. Without access to the right data at the right time, SecOps teams have greater risk exposure, and ITOps and engineering teams struggle to prevent critical issues.

"The rapid pace of digital transformation has left many organizations with siloed tools across their hybrid, multicloud architectures, stranding operations and development teams on separate islands with no context or visibility upstream or downstream. This technical debt of niche tooling has handicapped SecOps and ITOps' ability to gain context-rich insights required to keep the most mission-critical, customer-facing applications securely up and running."

— Cory Minton, Field CTO, Splunk

Technology executives cite their toughest obstacles to managing downtime



Testing new technologies carries some risk, some reward

Forty-three percent of technology respondents admit their development team often goes outside the approved tech stack to deploy new technologies (e.g., through “shadow IT”), which could trigger more downtime and severe security incidents.

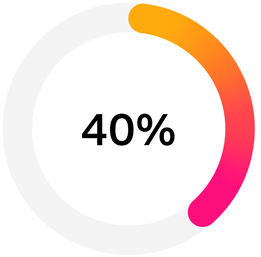
Because organizations often need to strike while the iron is hot, 78% of technology respondents say their organization is willing to accept downtime risk to adopt new technologies. But it doesn’t have to be this way. Planned downtime is common in highly regulated industries. For example, the financial sector, which adheres to an industry standard of 99.9% uptime, executes downtime to accommodate new feature launches at off hours to affect the fewest customers.

Deterring downtime in the era of AI

Security, ITOps, and engineering executives claim their organizations use an average of six tools to find and fix the root cause of a downtime incident. And the suite of tools is expansive. From application and cloud security to network and database monitoring, roughly two-thirds of tech executives say all tools mentioned in our survey are “helpful” or “extremely helpful.”

But no other technology has made as much of a splash recently as generative AI: 65% use discrete generative AI tools to address downtime. Among that group, 74% claim they see a considerable benefit. These tools can equip smaller teams with the information needed to mitigate downtime and get back online quickly. However, their use should always align with an organization’s corporate governance policy so practitioners don’t inadvertently expose intellectual property.

Weighing speed vs. security



Of CMOs say speed-to-market is more important than security and reliability

Complexity in the infrastructure and architecture of the application, coupled with a high demand for pushing innovation out quickly to customers, leads to a perfect storm of human error.

— Mala Pillutla, GVP of Observability, Splunk

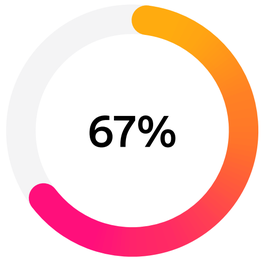
“Enterprises are investing heavily in generative AI, but threat actors are equally motivated.”

— Poonam Khemwani, Executive Director, IT and Cloud Security Architecture, JPMorgan Chase

Meanwhile, over half of technology respondents use generative AI features embedded into existing tools to address downtime, with 64% claiming they already reap significant gains. Some of the most helpful generative AI features we’ve seen are domain-specific chat experiences (AI assistants) that help write queries and troubleshoot.

According to Splunk’s State of Security 2024 report, executives and practitioners are optimistic about using generative AI for cybersecurity use cases — such as risk identification and threat detection/prioritization — which could drastically reduce cybersecurity-related downtime. We’re excited to see what the future holds.

Generative AI will increase downtime



Of technology respondents say downtime will increase due to cybercriminals and threat actors using generative AI

Generative AI use cases to address downtime range from generating a summary of detections to assisting in troubleshooting and remediation.

— Hao Yang, VP of Artificial Intelligence, Splunk

Resilience leaders know the ropes

“Being a resilience leader means being able to sleep at night knowing the business will keep running even when the unexpected happens — and knowing that you’ve planned for problems and have effective processes in place to address them.”

— Greg Leffler, Director of Developer Evangelism, Splunk

Resilience leaders bounce back faster

What sets an organization apart when it comes to mitigating and recovering from downtime? Despite the majority of technology respondents claiming that their cybersecurity programs and observability practices are mature, the data doesn't lie.

The top 10% of organizations — who we define as resilience leaders[5] — suffer less frequent downtime, lower total direct costs, and minimal impact from hidden costs. And their common traits provide a blueprint for other organizations.

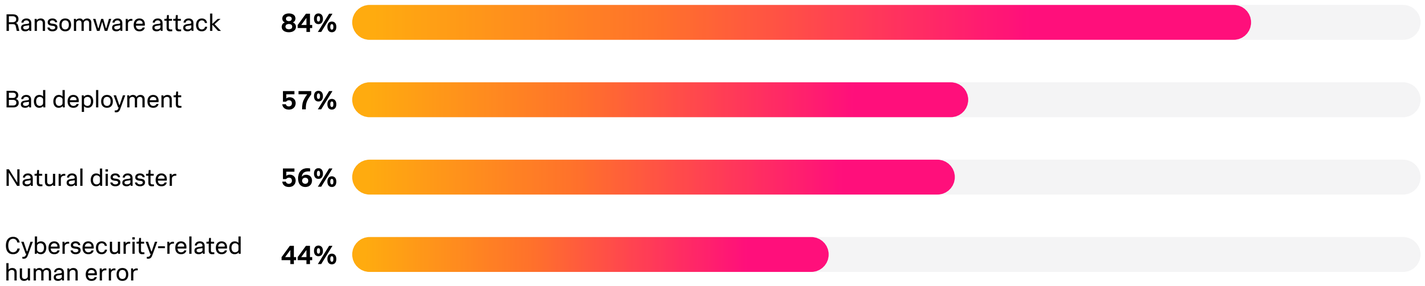
"Systems degradation is not an unknown occurrence. Systems outage is actually very, very rare because we spend phenomenal amounts of effort and money on operational resilience to make sure that systems are available and operational."

— Chris Russell Miller, Head of IT and Cyber Risk, BNP Paribas Personal Finance UK

Resilience leaders recover faster from downtime. On average, their mean time to recover (MTTR) from application or infrastructure-related downtime is 28% faster than the majority of respondents. And from cybersecurity-related incidents, it's 23% faster.

Faster recovery translates to a better customer experience, less unwanted media attention, and fewer dissatisfied end users.

Resilience leaders fix problems faster than non-leaders

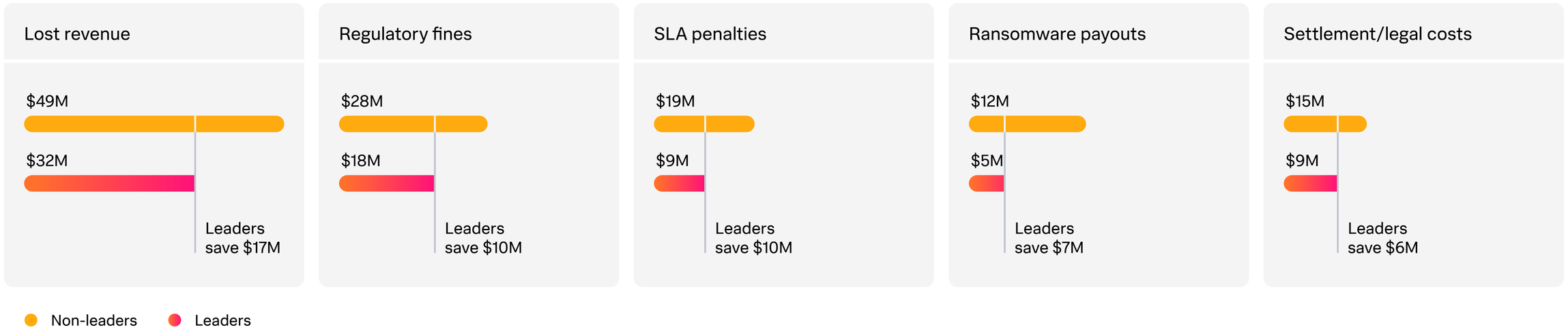


5 Resilience leader organizations were calculated based on frequency of downtime and amount of economic damage experienced from hidden costs.

Resilience leaders dodge the most damage

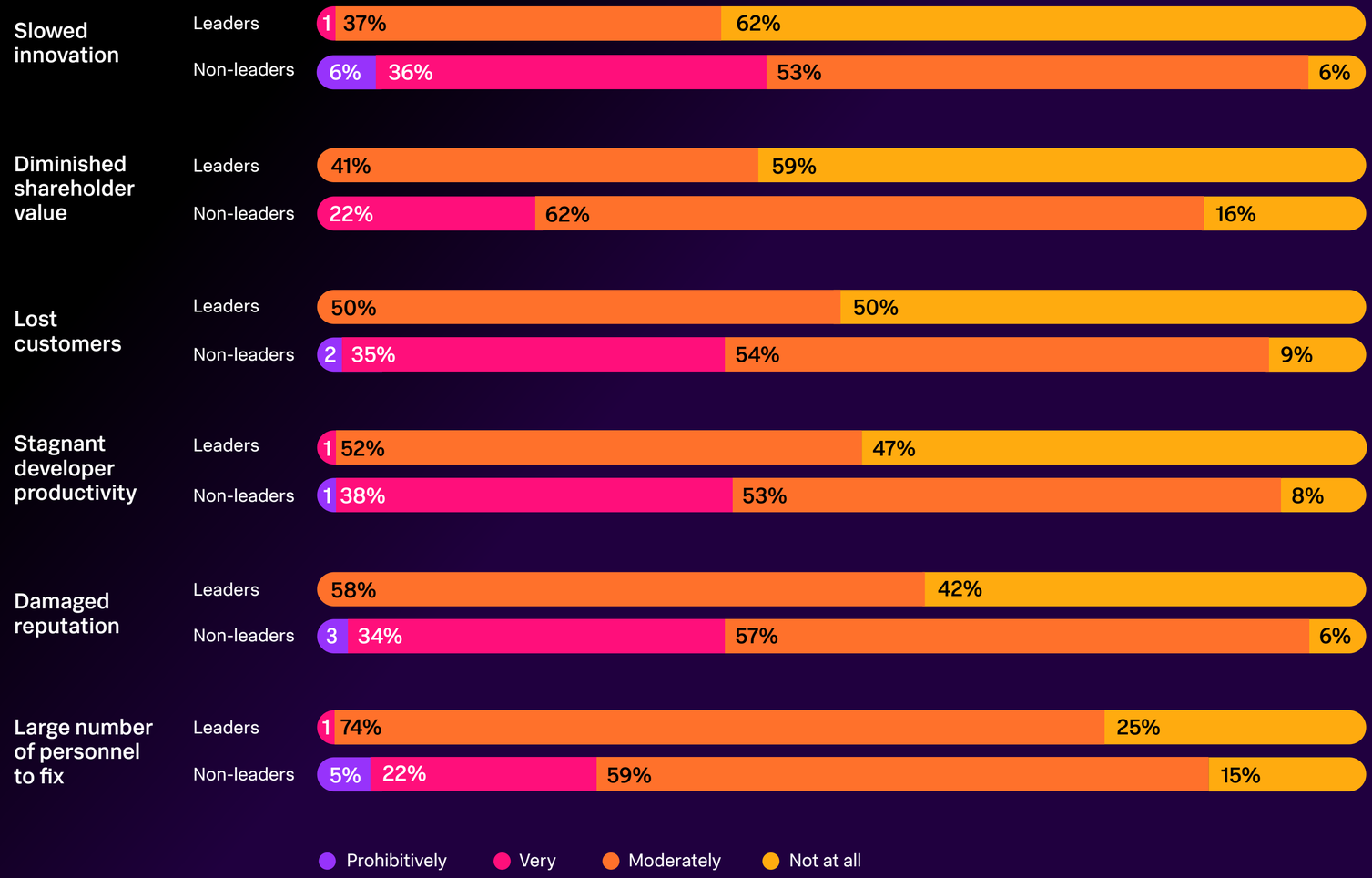
Leaders experience 245 hours less application or infrastructure-related downtime per year than non-leaders. And on the security side, they suffer 224 hours less. Resilient organizations minimize the financial setbacks of downtime in direct costs and feel less pain from hidden costs.

The direct costs of downtime are lower for resilience leaders



Resilience leaders feel less toll from hidden costs — none of them describe the economic damage as “prohibitive.” Most leader organizations experience no damage or describe it as “moderate.” Compare that with the remaining 90% of organizations that call hidden cost impacts “moderately” or “very” damaging.

The hidden costs of downtime are less damaging for resilience leaders



Percentages may not add up to 100% due to rounding.

Resilience leaders look ahead

Resilience leaders are more mature in their adoption of generative AI, expanding their use of discrete generative AI tools at five times the rate of non-leaders and at four times the rate for generative AI features embedded in existing tools.

But generative AI isn't the only forward-looking investment resilience leaders make. On average, this group invests $8M more in additional infrastructure capacity, $11M more in cyber insurance premiums, and $10M more on backups than non-leaders.

Resilience leaders also spend $12M more on cybersecurity tools and $2.4M more on observability tools. When asked if their current tool spend is adequate, leaders are more likely to say "no," leading us to believe they better understand downtime's broader business effects and recognize that addressing it is an evolving challenge.

All this talk on spending begs the question: Does being a resilience leader simply require more budget? Not necessarily.

We believe leaders invest smarter, not just larger. The emphasis on data management and tool consolidation will lead to more innovative security and observability strategies. Meaning, fewer investments with improved outcomes like comprehensive visibility and cross-collaboration, enabling a proactive approach to downtime.

Resilient organizations understand the financial consequences of downtime. They see what's above and below the surface and deliberately invest to prevent it from happening in the first place. Thankfully, the vast majority of tech respondents admit that the negative impacts they experience from downtime are unacceptable. We're heading in the right direction.

You can throw money at problems all day and not fix them. Being a resilience leader is about having a mindset that downtime isn't acceptable — and building systems, processes, and practices that enable that.

— Greg Leffler, Director of Developer Evangelism, Splunk

Resilience leaders recognize their AI-driven future

Leaders – extent of generative AI use

Using discrete generative AI tools:

Using generative AI features within existing tools:

Non-leaders – extent of generative AI use

Using discrete generative AI tools :

Using generative AI features within existing tools:

Not started · Considering · Piloting · Expanding

Percentages may not add up to 100% due to rounding.

Navigating downtime at your organization

“Digital resilience is not just about mitigating downtime. It’s about thriving in today’s world.”

— Mala Pillutla, GVP of Observability, Splunk

Pro tips for strengthening resilience

In a more resilient world, yes, organizations will grow short-term profits. But they'll also build longer-term value. Nearly half of security, IT, and engineering executives declare their downtime unacceptable. Companies understand there's too much at stake, both for themselves and for their customers. From corporations to critical infrastructure, securing consumer and investor confidence is table stakes.

But with varying budgets, regulations, and regional infrastructure, executives struggle to steer clear of downtime and its costly consequences. That's why we've provided our recommendations for championing a more resilient business.

1. Have a downtime plan.

Downtime is inevitable, so it's essential to have the proper procedures and tools in place. Instrumenting every app, following a runbook for outages, and identifying owning engineers — and ensuring everyone knows who's on point — is good corporate hygiene. To strengthen your plan, perform regular tabletop exercises with your SecOps, ITOps, and engineering teams, running through hypothetical scenarios to practice and verify responses to downtime events. Or, consider adopting "chaos engineering," real drills that build a more resilient system.

2. If you're not performing postmortems — you should.

Want to stop repeat issues that create downtime? Root cause analysis during incident response can single out the underlying problem and point to a fix. Invest in observability tooling and integrate data from across your environment into one centralized location so it's easier to isolate root causes. Eliminating silos and easily accessing data across tools lead to rigorous postmortems that will avert repeat occurrences.

3. Keep calm and protect your company IP.

Inputting company IP into any large language model (LLM) comes with security risks. Establish a clear data governance policy to safeguard your organization from data leakage. But keep in mind: Discrete generative AI tools are just the beginning. Opt instead for generative AI features embedded into existing tools — like generative AI chat assistants — to help address downtime. These domain-specific assistants can improve productivity and elevate employees' skill sets, benefiting your organization in the long run.

4. When you connect your teams and tools, everybody wins.

Downtime comes from anywhere. That's why complete visibility across SecOps, ITOps, and engineering is critical. Teams that share tools, data, and context will have an easier time collaborating, fixing the problem, and identifying the root cause when downtime occurs, allowing you to get back up and running quicker.

5. A proactive approach to downtime helps fireproof your organization.

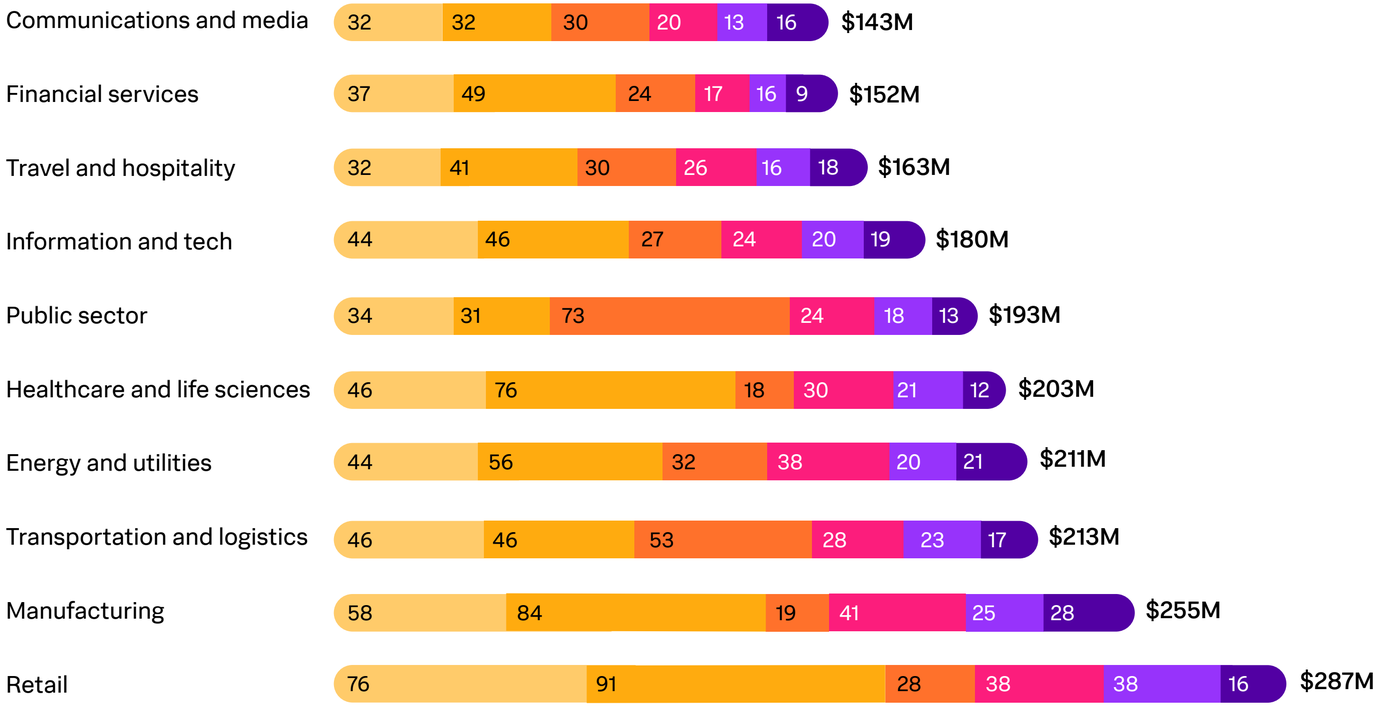
Getting ahead of issues is a cornerstone of digital resilience. Empower your SecOps, ITOps, and engineering teams with a proactive and collaborative downtime prevention program by investing in AI- and ML-driven solutions for pattern recognition. Predictive analytics powered by AI are a force multiplier that helps prevent issues from becoming five-alarm fires.

Downtime looks different in every industry

Although each industry suffers about the same amount of downtime, the costs of that downtime vary.

It's apparent that no other industry suffers more from downtime than retail. But what's not apparent are industry interdependencies. When banks are down, so is just about everything else. In effect, downtime in financial services generates downtime in other industries. When manufacturers are down, it upends every aspect of the supply chain and downstream organizations like retailers and logistics companies. Likewise, downtime in communications and media interferes with retail and banking. However, the most troubling effect of downtime in communications and media is that it may prevent citizen access to emergency services or hinder the coordination of disaster recovery.

Downtime costs add up for every industry



Cost category detail in $M:

Lost revenue	
Contractual/legal	Regulatory fines, SLA penalties, settlement/legal costs
Damage control	Brand trust campaigns, PR/investor relations
Security lapse costs	Ransomware payouts, cyber insurance premiums, extortion payouts
Staffing/productivity	Overtime wages, lost productivity
Upgrade needs	Additional infrastructure capacity, recovering from backups

The costs of downtime around the world

Geography plays a role in the costs of downtime due to factors like regulatory environment and digital infrastructure. In fact, 89% of technology respondents say the quality of digital infrastructure in their organization's country impacts downtime occurrences.

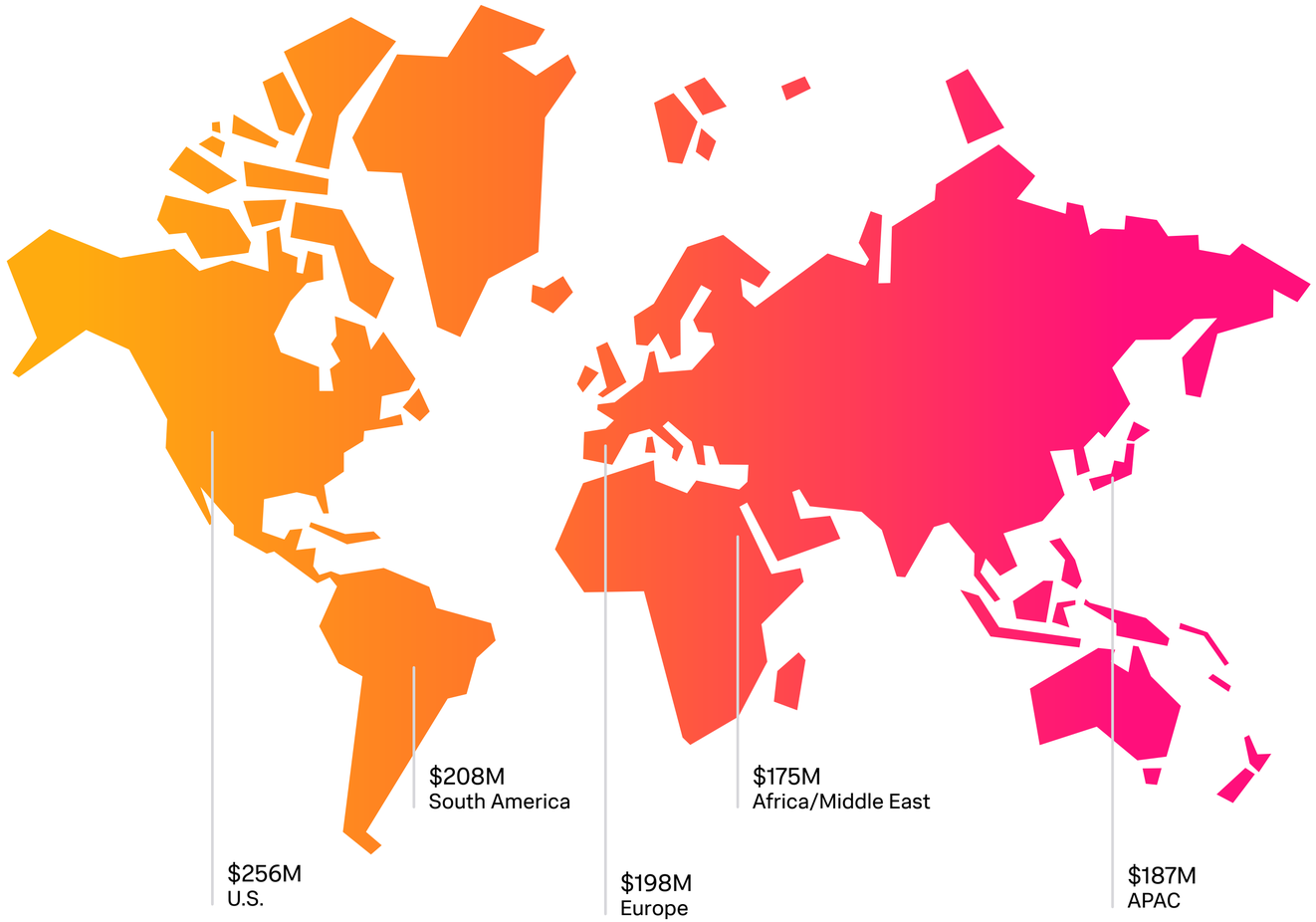
Downtime is pricier for U.S. companies than their global counterparts, primarily due to direct loss of revenue ($68M) and penalties for missed SLAs ($27M). U.S. companies also pay more in settlement/legal costs ($19M) and cyber insurance premiums ($14M). The U.S. also spends more on additional marketing activities ($31M total) post-incident.

Organizations in Europe — where workforce oversight and cyber regulation tend to be stricter — report the same costs for regulatory fines ($29M) and lost employee productivity ($11M) as the U.S. However, Europe pays more in overtime wages ($12M) and recovering backups ($9M).

Although they have the lowest overall costs, Africa and the Middle East spend the most on ransomware payouts ($22M) and extortion payouts from ransomware attacks ($12M).

Geography also shapes how quickly an organization's brand health, revenue, and stock price recover post-incident and remediation. Europe and APAC hold the longest recovery times, while companies located in Africa and the Middle East recover the fastest in all three categories.

If you're located in the U.S., expect downtime to cost you more

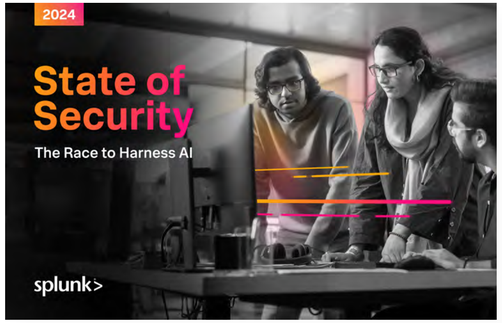


Strengthen your digital resilience with Splunk

Perspectives by Splunk — by leaders, for leaders

Looking for more insights on executive strategy, cybersecurity, and observability trends? Learn how leaders tackle today's most pressing challenges including AI, emerging threats, and the changing compliance landscape.

Learn more



Join the race to harness AI

The path to digital resilience is fraught with challenges for security leaders, none greater than AI. Learn how your organization can wield AI's power and prepare to defend against it.

Get the report

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 53 countries are represented from Africa, APAC, Europe, the Middle East, North America, and South America. Respondents hail from 10 industries: energy and utilities, financial services, healthcare and life sciences, information services and technology, manufacturing, communications and media, public sector, retail, transportation and logistics, and travel and hospitality. Respondents come from technology (including security, IT, and engineering titles), finance (including Chief Financial Officers), and marketing functions (including Chief Marketing Officers).

How Oxford Economics calculated the costs of downtime

Oxford assessed the costs of downtime for the Global 2000 by adjusting survey responses to match the characteristics of the Global 2000 in 2023. They used survey responses to estimate downtime costs relative to revenues (i.e., as a percentage of revenues to adjust for differences in company size among respondents), calculated the typical cost per unit of revenue by taking the median of the previous metric for each country in the study sample, and then combined revenue data from fiscal year 2023 for each company in the Global 2000 with the median value for the corresponding country. This scaling process helped align the survey responses with the size and regional distribution of Global 2000 companies.

About Splunk

Splunk, a Cisco company, helps make organizations more digitally resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent infrastructure, application, and security incidents from becoming major issues, recover faster from shocks to digital systems, and adapt quickly to new opportunities.

Keep the conversation going with Splunk.

splunk>

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.

24.CMP.report.the-hidden-costs-of-downtime_v12