The State of Resilience 2025

Confronting Outages, Downtime, and Organizational Readiness

CockroachDB

Executive summary

What 1,000 senior cloud and technology executives from all over the world are saying about their organization's operational resilience — and their strategies for increasing it

Outages happen. Despite almost universal awareness of this fact, a shocking majority of businesses find themselves dangerously exposed to serious consequences when an outage occurs.

Fallout following the recent CrowdStrike global outage jolted many organizations into action — 94% of technical executives in this survey said that the event has catalyzed their companies to reassess their operational resilience. At the same time, leaders at the global enterprise companies surveyed here, in "The State of Operational Resilience 2025," report that entrenched resistance to change, misaligned internal priorities, outdated systems, and budgetary gridlock prevent many from implementing meaningful — sometimes even desperately needed — operational resilience measures.

1. Leaders are worried: 93% of leaders are concerned about the financial and organizational impacts of outages, and **95% are aware of operational weaknesses that leave them vulnerable**. At the same time, however, 48% say their organizations aren't doing enough to improve resilience.

2. The high cost of service disruption: 100% of companies surveyed experienced revenue losses from outages in the past 12 months with per-outage losses ranging from at least US$10,000 to well over $1,000,000.

The data also shows that the larger the organization, the larger the annual revenue loss. For companies over 1,000 employees and/or US$500 million ARR, outage-related losses averaged US$495,000 — though a **handful of of these large enterprise organizations (8%) reported losses of US$1 million or higher over the last 12 months**.

3. Outages are the new normal: On average, companies report 86 outages per year—translating to 324 minutes of weekly downtime. 55% experience weekly outages, while 14% report daily outages.

53% of banking and financial services companies report experiencing service disruptions at least weekly, as do 60% of retail and ecommerce enterprises.

These are not minor incidents. **70% of large enterprise companies**[1] **report that their outages typically take 60 minutes or more to resolve**. Overall, nearly half of all respondents report that their average downtime lasts two or more hours before resolution, with 10% reporting the loss of a full workday or more before they are able to resume operations. **The average outage time across all geographies, ARR, company sizes, and industries is 196 minutes – or more than three hours of service disruption**.

[1] *Defined for this report as organizations with more than $500m ARR and 1,000+ employees*

4. Unplanned outages cause more than economic losses: Externally, they cause the loss of consumer and business partner confidence, damaging the organization's reputation. Internally, they diminish trust in the technical IT responsible for preventing or mitigating outages. An engineering group lacking the trust of the larger organization will have a difficult time recruiting and retaining quality technical staff.

Frequent outages also cause a risk of staff burnout and high turnover when teams are forced to miss other deadlines (39%) and pile up a backlog of requests (43%) — while staying later or working weekends (48%) — to fire-fight outages.

5. Preparation is spotty: Only 20% of respondents describe their organization as fully prepared for outages. Only 33% have an organized response approach, and less than a third conduct regular failover testing.

6. Resilience investments are overdue: Many organizations have known weaknesses, with 49% planning to invest in automation, AI, and cloud infrastructure to boost resilience.

7. New operational resilience regulations loom large: A majority of all the technology executives surveyed (79%) admit their organization is not completely prepared to comply with new operational resilience governance regulations like DORA (going into effect in Jan 2025) and the NIS2 directive, opening them up to consequences. Nearly half (44%) say they are losing sleep over the regulatory fines and penalties that come from unplanned downtime or outages.

Executives in EMEA (Europe, the Middle East and Africa) (85%) are more likely than executives in APAC (Asia-Pacific) (76%) and North America (75%) to admit not being completely prepared to comply with new regulations regarding unplanned downtime and outages.

Survey Methodology

The Operational Resilience in Enterprises Survey was conducted by Cockroach Labs and Wakefield Research among 1,000 Senior Cloud Architects, Engineering, & Technology Executives, with a minimum seniority of Vice President in three regions: North America (US, Canada), EMEA (Germany, Italy, France, UK), and APAC (India, Australia, Singapore), between August 29th and September 10th, 2024, using an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 3.1 percentage points in the global sample, 6.9 percentage points in the United States, and 9.8 percentage points in each of the remaining markets from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

Introduction

Just a few months have passed since the biggest global software failure to date. The CrowdStrike outage damage was widespread and instantaneous: As millions of devices crashed, millions of banking customers were cut off from their accounts. Airlines grounded flights by the thousands, hospitals canceled surgeries, and universities canceled classes. Emergency police, fire, or medical aid became unavailable in some areas as 911 call centers went offline. The cause of this global disaster was every technologist's worst nightmare: a single faulty section of code in a single software update from a single company.

How can you ensure your company is prepared for next time?

We conducted this survey because operational resilience has, until now, been generally overlooked. Most companies focus on disaster recovery (DR), which is important after disruptions occur. However, operational resilience focuses on preventing service interruptions before they happen.

In today's astonishingly complex technical architectures, with their interdependence of sophisticated digital services, anything that can go wrong, will go wrong eventually. The results of this survey bear this out: 100% of companies surveyed experienced revenue losses from outages in the past 12 months, with per-outage losses ranging from at least US$10,000 to well over US$1,000,000. Across all sizes and sectors, the enterprises in this survey experience, on average, 86 outages per year; the average length of an outage is 196 minutes — over three hours of downtime.

These numbers, startling as they are, still don't represent the true cost of downtime. These figures do not include any additional fines or penalties that may be levied as part of new operational resilience regulatory actions in the EU and beyond. Fines that can easily double the initial costs of the outage itself, and — because these regulations carry the force of law — allow government entities to penalize out-of-compliance companies and can dictate how, and even if, a company is allowed to operate. The numbers also fail to represent the reputational damage a company will experience, following a major outage — including potentially a decrease in stock value when investor confidence gets rattled.

As the data from this survey demonstrates, outages carry more than financial costs, and can cause long-term repercussions. These seasoned technical leaders from every type of industry and from all around the globe divulge the current state of operational readiness in their own organizations — and their strategies for increasing their operational resilience without introducing new risks.

The report in six parts

Outages happen. Yet data collected in this survey reveals that, **despite almost universal awareness of risks, a majority of businesses find themselves dangerously exposed to serious consequences when an outage happens**. The CrowdStrike outage has jolted organizations into action, yet entrenched resistance to change, misaligned priorities, outdated systems, and budgetary gridlock prevent many from implementing meaningful operational resilience measures. This report is in six parts:

Part 1: Operational resilience in 2025 reveals the current state of operational resilience in 2025. How often do organizations experience outages? What are the common causes behind this downtime, and what exactly are the financial and operational impacts when a service disruption happens?

Part 2: Enterprise disaster readiness queries how companies respond to outages, and how they work to prevent them in the first place. What challenges do they face when tasked with improving their organization's operational resilience, and what factors potentially block their progress?

Part 3: The road to resilience is a look at the tactics companies use to prevent unplanned downtime and service outages and their strategies for making improvements. Where are organizations targeting new investments aimed at increasing their current operational resilience?

Part 4: Operational resilience and regulatory risks examines the average organization's readiness to comply with new legal mandates around operational resilience and ability to comply with data privacy regulations in the event of data loss or corruption following an outage.

Part 5: Key takeaways and emerging enterprise operational resilience strategies summarizes this report's findings. What do they mean for technical leaders trying to operate in a business-as-usual environment that's far more complex than ever before, while implementing positive changes without introducing new risk?

Part 6: How distributed SQL helps organizations achieve operational resilience uses data points and takeaways from this report to show how distributed application architecture helps enterprises increase their organizational resilience by mitigating the technical risks and weaknesses that lead to outages.

PART 1

Operational resilience in 2025

Are tech leaders worried about their operational resilience?

In a word, yes — and for good reason.

1.1 Real-world outage costs & impacts

100% of the technology executives surveyed in this report say that their company lost money due to outages over the past 12 months.

Dollars down the drain

In the past twelve months, across all companies of all sizes and annual revenues in all sectors, **one-third (32%) of respondents lost US$100K or *more* due to outages**.

And, the bigger the player, the bigger the penalty: **companies with higher revenue (US$500m+) are 256% more likely to incur outage-related financial losses of over US$1M per year**. On the surface, this reflects the fact that more people are impacted when a larger company suffers an outage — but it also illustrates just how high the financial stakes can be.

Losing more than money

100% of organizations in this survey say that outages have had significant negative impacts on their technical teams and staff.

Drop everything: Beyond causing financial losses, unplanned downtime or outages disrupt normal business operations in other ways. In fact, **92% of the executives surveyed report their teams must occasionally deprioritize essential work in order to address unplanned downtime or outages**. Two thirds (66%) say they are forced to deprioritize everyday tasks like improvements, maintenance, or administrative tasks frequently or even all the time.

Fear of firing: An overall 82% of leaders surveyed (87% in the US and APAC; 77% in EU) expressed **fear that they or members of their technical teams could lose their jobs following a significant outage or downtime event**.

Fire-fighting fallout: Beyond dropping workday responsibilities to fire-fight an outage, an overall **48% of executives say their teams also must work overtime and on weekends** to fully restore normal operations. **The same number (48%) also say that unplanned downtime has derailed their tech teams from meeting objectives** — which, in turn, creates even more unplanned work required to prepare for and conduct post-mortems and investigations (39%).

Stressed technical teams: Not surprisingly, this frequently leads to friction and finger-pointing among technical teams (43% overall, 48% in North America). **The majority of respondents (91%) say that overtime and increasing work backlog due to outages are a significant stress factor on their teams**, which in turn can lead to potential burnout and higher turnover.

1.2 Outages by the numbers: frequency & duration

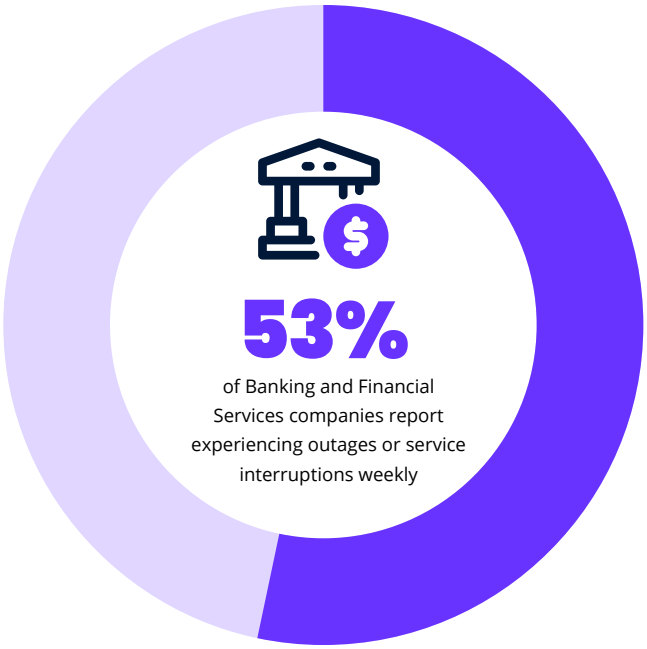
100% of respondents report experiencing unplanned, unexpected downtime in the past 12 months.

Despite unanimous recognition that outages cost companies both financially and organizationally, the data gathered for this report shows that unplanned downtime and service outages are not isolated incidents. **A significant majority of companies (69%) experience outages/ service interruptions *at least weekly***. For about one in seven companies (14%) outages are a daily occurrence.

53% of Banking and Financial Services companies report experiencing outages or service interruptions weekly or more often – as do 60% of Retail/Ecommerce companies

Time is money. The clock is ticking when an outage occurs; it's a situation where time is literally money down the drain. Stunningly, **when an outage happens, overall average downtime is 151 minutes** time to recovery (TTR)[2] for resolving an outage (unless you're in India, where the average outage lasts 211 minutes).

Overall, just 2% of companies surveyed say they are able to resolve an unplanned outage in 60 seconds or less.



[2] *Time to Recovery (or Time to Resolution) is the full time of an outage — from the time the system or product fails to the time that it becomes fully functional again so that normal business operations can resume.*

1.3 The worries keeping tech leadership awake at night

93% of executives in this survey say they are losing sleep over the impacts of unplanned downtime.

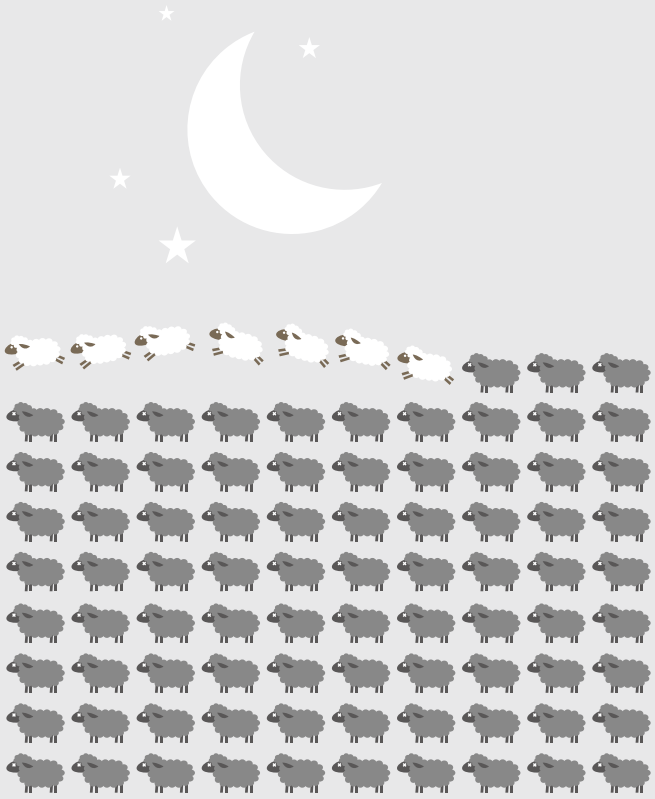
And the data gathered for this report show that they have good reason: **86% say that every minute of unplanned downtime is a minute they risk losing customers, perhaps permanently**. Beyond the obvious financial fallout, there are many other sources for executive anxiety as well:

- **Regulatory retaliation:** 44% overall (85% in EMEA) are worried about the regulatory fines and penalties that can be levied when an outage occurs – which can go as high as €5,000,000 (approximately US$ 5.5 million) — and the risk that regulatory authorities can limit a non-compliant entity's ability to conduct business until they comply.

- **Data disaster:** One out of every three leaders (36%) worry about data getting corrupted, or even completely lost/destroyed, during unplanned downtime. Data loss haunts SMB startups and venerable global enterprises alike: this percentage is remarkably consistent regardless of company size, longevity, revenue, or location.

- **Potential punishment:** 82% of leaders acknowledge that their teams are worried technical staff will be fired for unplanned downtime or outages. These numbers are higher still at companies experiencing more frequent (several times per month or more, 88%) outages, or where average outages lasting a significant amount of time (two hours or more, 88%).

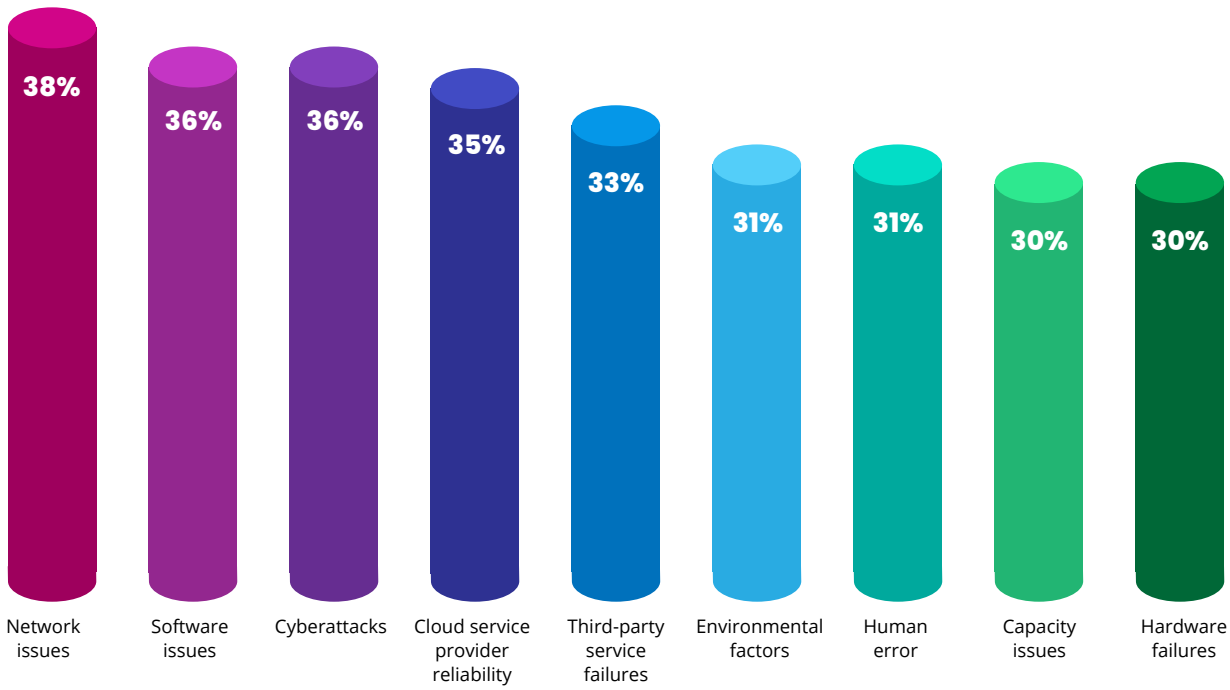
- **Career concerns:** Almost half (44%; 49% in NA) worry that unplanned downtime erodes internal trust in their technical teams and leadership. This lack of confidence from the C-suite, in turn, impedes their ability to get crucial buy-in for investing in infrastructure improvements.



93% **of executives in this survey say they are losing sleep over the impacts of unplanned downtime.**

1.4 Causes of downtime

> The breathtaking technical complexity of modern applications means that a multitude of faults can act as the root problem behind any outage or unplanned downtime — and that the cause can lie both inside and outside of the afflicted organization.



Interestingly, the *frequency of occurrence* of the causes behind the outages respondents have experienced were remarkably consistent across all cohorts examined in this survey, regardless of company revenue, size, longevity, or location.

This is good news, actually. **When the root causes of downtime strike so similarly and consistently across the board, the solutions and strategies for defeating downtime and improving operational resilience will be equally consistent for every organization, everywhere**.

PART 2

Enterprise disaster readiness

The current state of operational resilience challenges and response strategies

Are organizations more proactive or reactive when an outage happens? How are they working to prevent unplanned downtime in the first place?

2.1 The state of outage response strategies (or lack thereof)

Globally, 95% of the executives surveyed say they are aware of at least one existing, unresolved operational weakness within their technical estate that puts their organization at risk.

Nearly three-quarters (72%) say their organization has *multiple* operational weaknesses that impact their organization's ability to meet business and technical objectives.

Proactive vs. reactive organizations

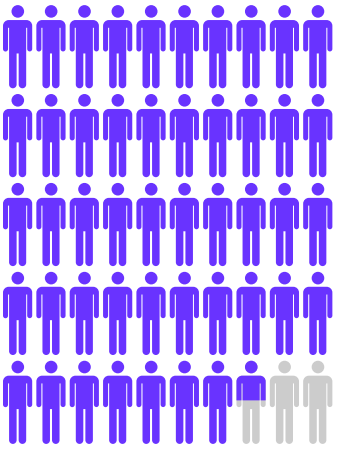
39% of executives describe their outage handling as "reactive." They respond to outages as they occur, with no formal protocols or response planning in place. Larger enterprises (1,000+ employees), though, are significantly more likely (49%) than smaller organizations and startups to have formal protocols and preventive measures like continuous monitoring in place to minimize unplanned downtime and service disruption.

Despite acknowledging the inevitability of unplanned downtime, these reactive organizations say they rely on a few key people to respond to and manage outages when they happen — essentially, a single-point-of-failure strategy.

Outage response strategies

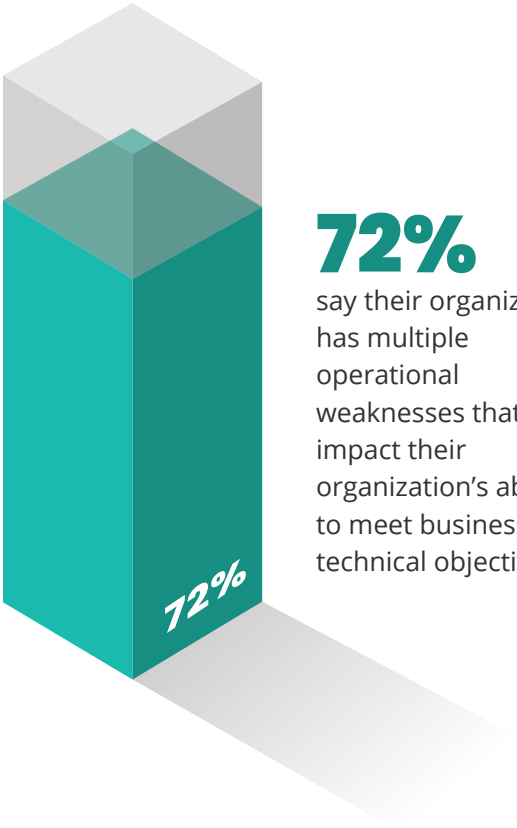
"Controlled" chaos: Regardless of whether they are proactive or reactive, most organizations (57%) report being only "moderately organized" when reacting to unplanned downtime or outages, and they recognize there are gaps in protocols that need to be addressed.

Reinventing the (broken) wheel: 10% of organizations describe their response to unplanned downtime or outages as "chaotic" — for them, it's a scramble to determine how best to address each new problem as it happens.



95%

of the executives surveyed say they are aware of at least one existing, unresolved operational weakness within their technical estate that puts their organization at risk



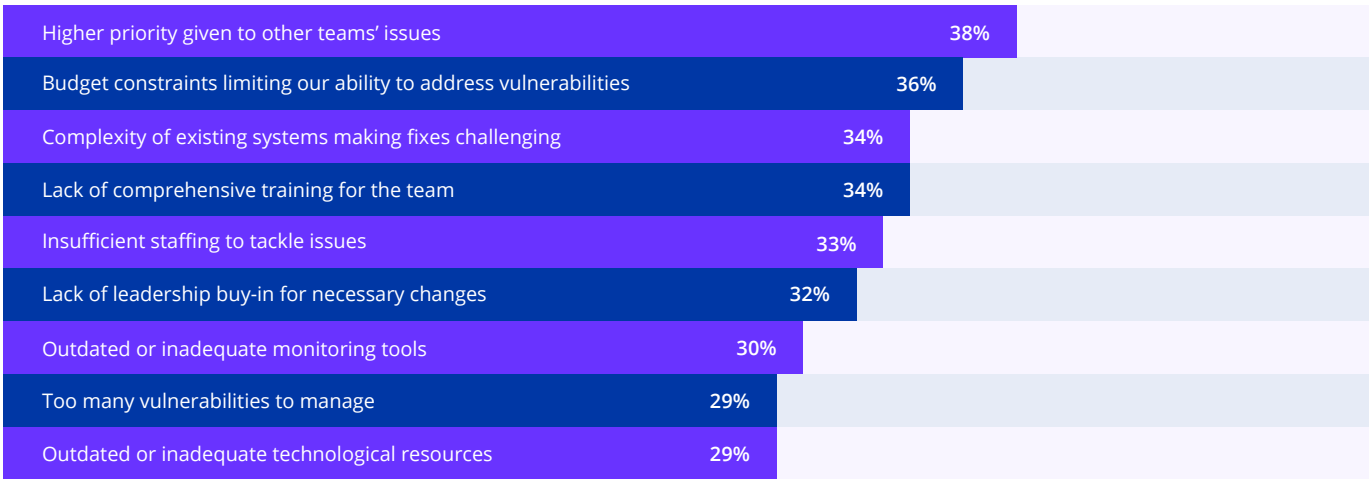
72%

say their organization has multiple operational weaknesses that impact their organization's ability to meet business and technical objectives

2.2 The challenges tech leaders report facing when tasked with improving operational resilience

94% of leaders worldwide admit that the CrowdStrike outage has forced them to reevaluate their business continuity strategies.

While leaders are saying almost unanimously that the global fallout from the CrowdStrike outage has catalyzed their organizations to get serious about implementing operational resilience strategies, some are worried that their company may not be able to change course.



A new sense of urgency

The call is coming from inside the house. Leaders worldwide say that fallout from the CrowdStrike has increased their organization's sense of urgency: overall, almost half (46%) say they are "significantly" improving planning, while another 48% are making "some" improvements.

But will anyone answer the call? Survey participants expressed mixed feelings about their organizations' ability to change course.

A full 50% believe their organization will increase their preparedness (and decrease their outage response times) over the next 12 months. Among the remaining half, 38% predict they will maintain the status quo. The situation is more dire for the 12% of executives that fear they will fall even further behind the operational readiness curve.

The factors blocking progress

Survey respondents say there can be significant obstacles and challenges in the way of improving their organization's resilience. What is blocking their progress?

- **Competing priorities:** The top reason that recognized vulnerabilities have not been addressed is because other teams' needs get prioritized instead (38%).
- **Financial constraints:** 36% report that budgetary challenges limit their ability to address vulnerabilities.
- **Lack of leadership confidence:** Those in charge may not be taking the issues as seriously as technical executives would hope: lack of executive leadership buy-in for their proposed solutions is a roadblock for 32%.

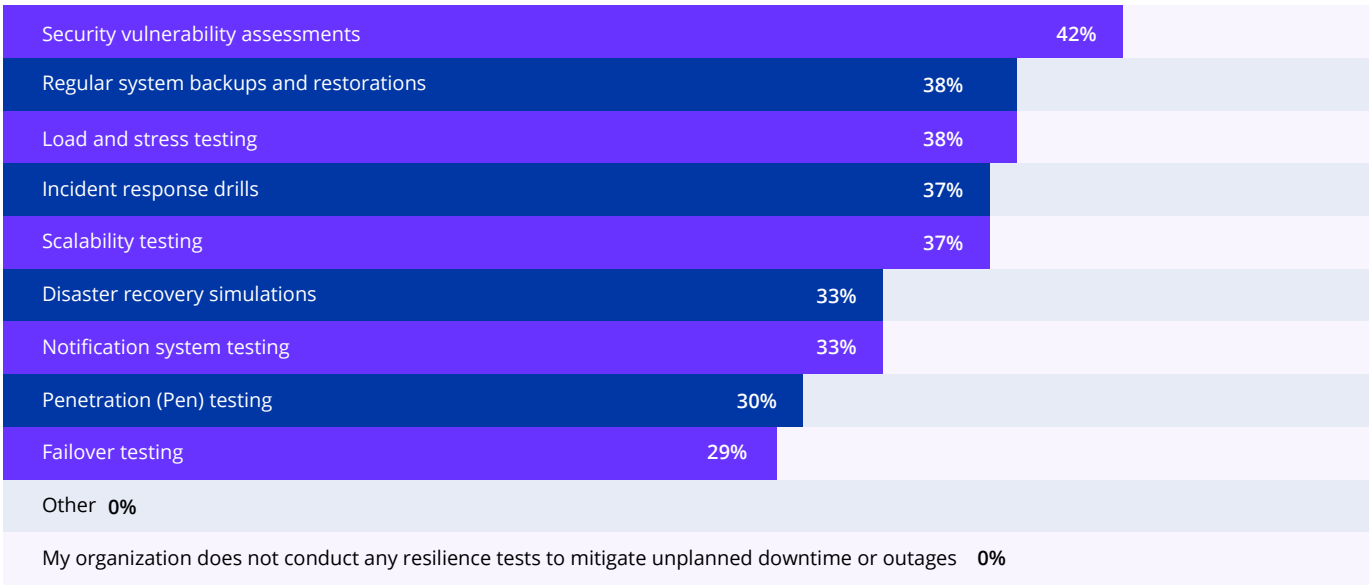
PART 3

The road to resilience

What tactics do companies use to prevent unplanned downtime and service outages, and what are their strategies for improving resilience?

3.1 How organizations report they are “doing” operational resilience now

Virtually all organizations (100%) conduct at least some sort of resiliency testing to mitigate unplanned downtime or outages.



Testing, testing

The tests conducted most often are security vulnerability assessments (42%), which help organizations protect their systems and data from unauthorized access and data breaches.

Other proactive assessments include regular system backups and restorations (38%) and load and stress testing (38%) to see how a system would respond under extreme conditions

Unforced errors

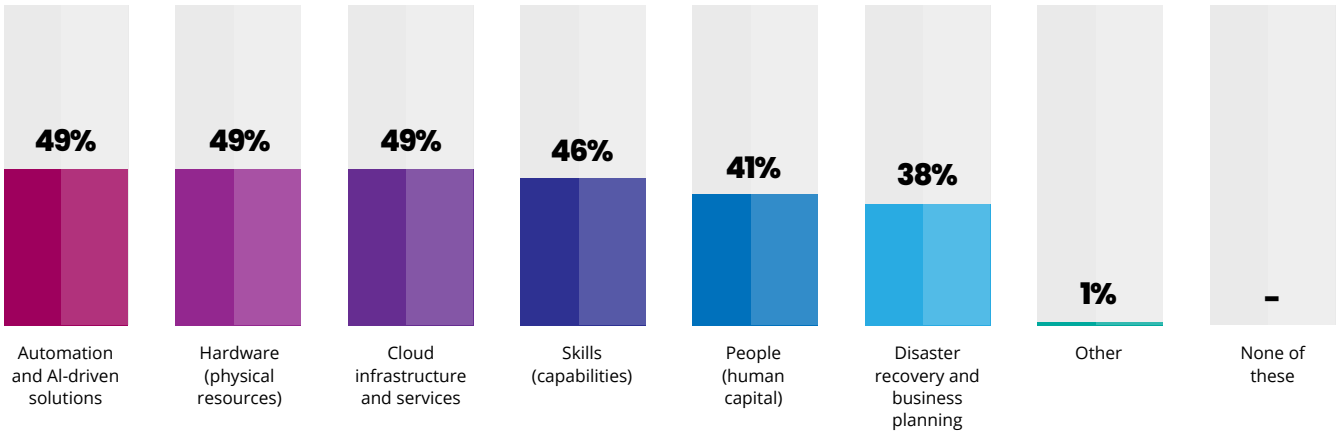
Some things are just basic best practices. But a surprising number of organizations admit they don’t always practice good technical hygiene when it comes to resilience fundamentals:

A shocking 62% of organizations in this survey fail to do regular system backups and restoration exercises.

71% do no failover testing to ensure their outage prevention protocols are working.

3.2 Where organizations are targeting future investments to increase their resilience

Overall, results show that organizations believe that no one area of investment is the most important for improving their operational resilience. These numbers are consistent across companies worldwide, regardless of whether they are long-established enterprises or smaller recent startups.



A multi-threaded path to prevention

Instead of focusing on a single approach, executives report pursuing a multi-threaded strategy of targeted investments in a variety of areas. Overall there is consistent agreement on the technologies that will benefit their continuity:

- **49%** believe they need to make more investments in their hardware to improve resiliency.
- **49%** also feel automation and AI-driven solutions would be valuable.
- **49%** believe their cloud infrastructure and services need additional investments.

Mind over machine?

In section 1.4, we saw that 31% of companies report experiencing an unplanned service outage due to human error.

People power for outage prevention: Overall, 46% of respondents believe they should be investing in training and skills within their organization. 41% are also looking to hire new headcount for positions to directly support operational resilience initiatives.

Automation through AI: Larger companies are more likely to be looking at AI solutions, especially if they are in the US or India, both locations where 57% of respondents indicate they are actively investigating AI-driven automation to increase the overall reliability of their systems.

A confluence of factors: Companies that say they are both (1) proactive in outage prevention and (2) committed to improving their operational resilience are the most likely to be investing in both human and artificial intelligence. This is a small cohort within the overall 1,000 leaders surveyed, but within this granular demographic respondents are significantly above average in seeking to increase their internal training (72%) and seeking automation and AI support to bolster their system reliability (68%).

PART 4

Operational resilience and regulatory risks

79% of technology leaders describe their org as “not completely prepared” to comply with new regulations regarding unplanned downtime and outages

It's no secret that operational resilience has been moving up the list of regulatory priorities for governments around the globe. Why? The probability of disruption — i.e., outages — and the potential impacts from those disruptions are both steadily increasing. Modern application architecture, reliant on digital technologies and third-party platforms and services, has simultaneously expanded the threat surface for disruptions. With no reason to believe any of these trendlines will reverse soon, regulatory authorities are stepping in to act.

The very real regulatory costs of downtime

Operational resilience is an increasing target of government legislation and regulatory efforts like DORA (the EU's Digital Operational Resilience Act) and the security-focused NIS2 Directive — and technology leaders are worried. DORA specifies the technical requirements aimed at ensuring operational resilience for financial institutions and critical services like utilities, logistics platforms, and healthcare. Similarly, the NIS2 Directive, a security-focused set of operational resilience requirements, spells out how organizations must implement technical, operational, and organizational measures to manage cybersecurity risks.

NIS2 became law for all companies operating in the EU as of October 2024; DORA regulations take full effect on January 1, 2025. Though these laws originate in the European Union, it's important to understand that **DORA and NIS2 cover any company operating in the EU in any form, even if they are headquartered outside of EU borders**.

No matter where they're based, it's not just financial services enterprises and those in other named sectors that need to worry. The regulations also cover third-party ICT (Information & Communications Technology) organizations: namely, digital and data services providers. Companies like CrowdStrike, for example, as well as cloud service providers, database companies, and other SaaS providers all face the same fines and penalties when they experience an outage.

These fines are potentially fierce: under DORA, financial entities and third-party ICT providers that are considered critical by the European Supervisory Authorities (ESAs) can be fined up to €5,000,000 or 1% of their global annual revenue, whichever is higher. NIS2 is even more punitive: the directive requires EU Member States to fine for a maximum of at least €7,000,000 or 1.4% of the global annual revenue, whichever is higher.

Beyond fines, other DORA/NIS2 outage-related penalties are also potentially severe. These include **operational restrictions**, where regulatory authorities can limit a non-compliant organization's ability to conduct business until they comply. EU member states can impose additional penalties, such as audits, suspensions, cease-and-desist orders, and public notices.

Even if an event escaped the widespread havoc of the CrowdStrike global outage, publicly documented DORA violations can still damage a company's brand and reputation. Beyond any customers lost as a consequence of an unplanned downtime incident, companies found to be in violation risk losing future customers — and investor confidence.

Technical leaders are worried. Very worried.

And for good reason. This survey — the first to examine enterprise readiness and concerns regarding regulatory compliance as these laws come into full effect — shows that many simply are not ready.

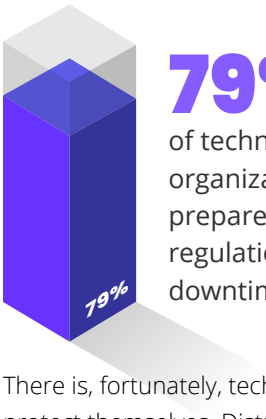
79% of executives overall say their organization as "not completely prepared" to comply with new regulations regarding unplanned downtime and outages, while 44% say they have "significant concern" over their organization's abilities to comply with operational resilience regulations.

Separately, 60% worry specifically about data loss or corruption occurring during an outage that could result in significant fines and penalties — not just under DORA and NIS2, but also GDPR and other data privacy regulations that impose penalties for data-related noncompliance.

How to get in compliance with operational resilience regulatory

DORA and NIS2 focus on mitigating the risks associated with disruption in essential or important digital services. GDPR and the alphabet soup of other current global data privacy laws (CCPA, PIPEDA, POPI, LGPD, HIPAA, PCI-DSS, to name but a few) focus on data integrity as an important component of overall operational resilience. Companies found to be out of compliance with these regulations can experience real and lasting consequences, both financial and operational — and no enterprise is immune.

It's not just the EU's DORA; there are many similar regulations on the horizon, from governments around the globe attempting to address operational risks, resilience, and business continuity. In the UK and Australia, new operational resilience requirements take effect in 2025. The governments of Hong Kong and Singapore are actively drafting new resilience regulations, while in the US representatives from the Federal Reserve, Treasury Department, and other agencies are currently developing a set of operational resilience standards as a blueprint for future legislation.



79%

of technology leaders describe their organization as "not completely prepared" to comply with new regulations regarding unplanned downtime and outages

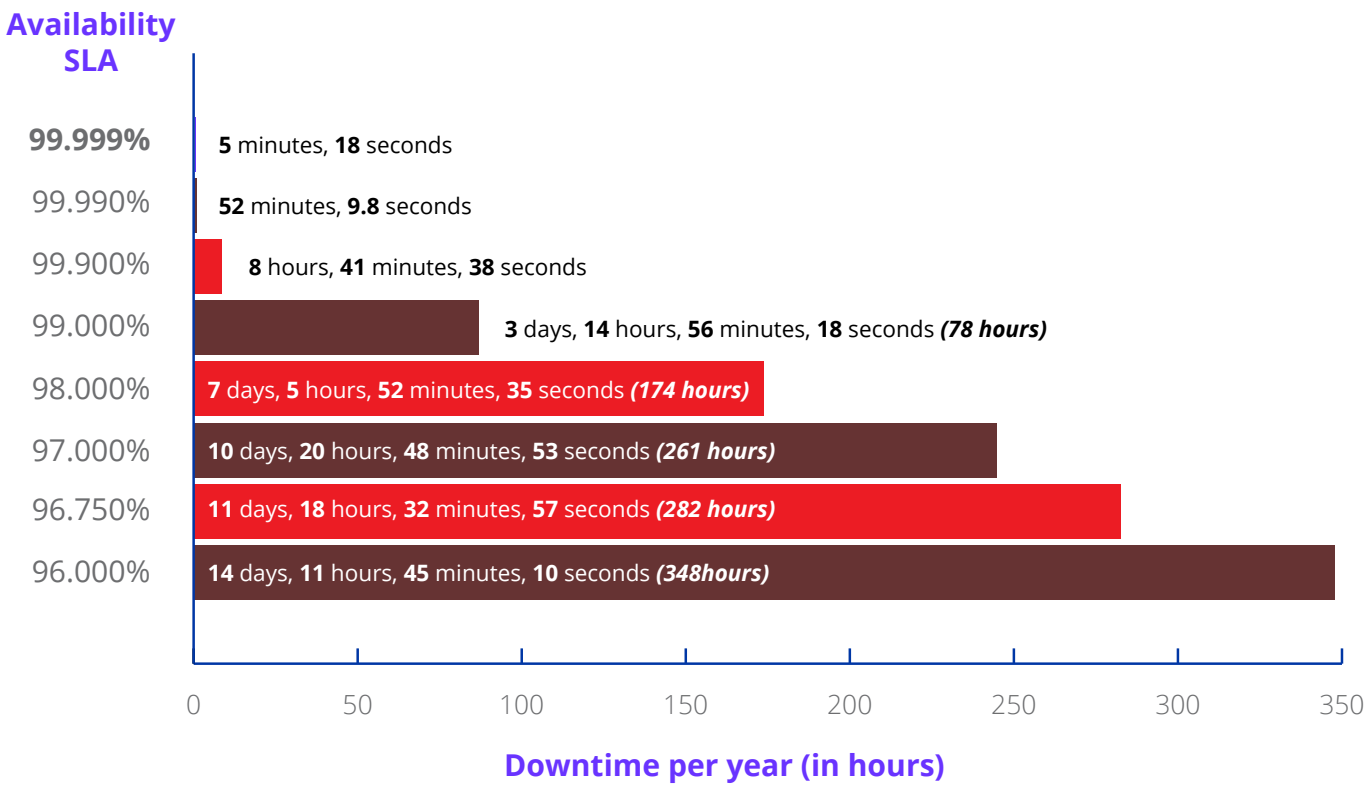
There is, fortunately, technology that can help enterprises protect themselves. Distributed systems, and particularly distributed SQL databases, significantly contribute to improving organizational resilience by mitigating the technical risks and weaknesses that lead to outages.

See the next section of this report ("How distributed SQL helps organizations achieve operational resilience") for information on how a distributed SQL database in particular can help organizations align with operational resilience regulations — and help companies achieve their overall operational resilience goals.

When "guaranteed uptime" is still downtime

A significant — and also very tactical — component of operational resilience lies in the service level agreements (SLAs) from each vendor regarding availability for services, platforms, or databases in your application stack. Availability SLAs are the percentage of time the cloud platform or database, etc, are operational. The goal is 100%, but even large and critical systems (such as the VISA card payments network or Amazon Web Services, for example) don't promise 100% availability. This is because when a modern cloud application processes thousands, even tens of thousands, queries per second, adverse events will inevitably occur. In the real world, the gold standard SLA is known as "five nines" or 99.999% uptime.

Results from companies in this survey show that they, on average across all organization sizes and sectors, experience 86 outages per year. The average outage lasts 196 minutes. This equates to an average of **280 hours of downtime** per year. This sounds like a lot of downtime — but it's actually within the limits of any service level agreement (SLA) guaranteeing 97% uptime.



A key tactic for improving operational resilience is, naturally, choosing solutions that offer the highest possible uptime.[3]

Using database-as-service (DBaaS) SLAs as an example, only two distributed SQL databases currently offer 99.999% uptime (5 minutes, 18 seconds per year): Google Spanner and CockroachDB. Both are globally scalable, synchronously replicated cloud native distributed relational databases that offer extremely high uptime SLAs out-of-the-box.

However, only one of them is truly fit for optimal operational resilience.

Spanner can only run on Google Cloud — which introduces a single point of failure for an application. A serious Google Cloud outage will take the database down along with it, even if the application itself is hosted on another ICP like AWS or Azure. CockroachDB, on the other hand, is cloud agnostic and can be deployed on any — or even all — of the major cloud providers, as well as self-hosted on premise and hybrid cloud/on-prem installations.

.

[3] *Calculation source uptime.is SLA and Uptime Calculator*

PART 5

Key takeaways and emerging enterprise operational resilience strategies

Priorities for changes to be made, and strategies organizations are considering

In 2025, ensuring operational resilience is no longer optional. It's imperative.

The cost of outages is high for companies. For 86% of executives, every minute of unplanned downtime is a minute they could lose a customer. Across all geographies, company sizes, and industries, the average annual outage-related revenue loss was US$222,323 over the past twelve months.

The findings from this survey of 1,000 global enterprise technology leaders highlight existing critical gaps organizations currently experience in terms of operational resilience within their digital estates. Despite near-universal recognition of the importance of uptime, many organizations remain dangerously vulnerable to the risks associated with unplanned downtime and outages. And, as new regulations like DORA and NIS2 come into effect (with others on the horizon), ensuring compliance and resilience has gone from something companies should do to something they must do — or face a very real risk of serious operational, financial, and regulatory consequences.

Key takeaways from this report emphasize both the urgency and complexity of addressing these challenges:

High frequency and cost of outages: A majority of enterprises face frequent outages, with 69% reporting service interruptions once or more per week, or even every day. These events are costly: overall, 32% report financial losses of US$100,000 or more annually. But the damage is more than dollars down the drain: 100% of organizations in this survey say that outages have had significant negative impacts on their technical teams and staff. Frequent outages can also cause lasting reputational damage, losing both customers and the confidence of both the C-suite and external investors alike.

Regulatory pressure is increasing: With 79% of organizations admitting they are not fully prepared to comply with operational resilience regulations, many executives are losing sleep over the potential financial penalties. This situation underscores the pressing need for improved resilience strategies to meet regulations like DORA and NIS2 — as well as the emerging legislative actions currently under consideration by governments around the world.

Automation, AI, and cloud investments: Essentially half (49%) of the respondents see investment in automation, AI, and cloud infrastructure as critical steps towards enhancing resilience. These technologies will help organizations improve system reliability, reduce human error, and recover more quickly from outages.

Emerging enterprise strategies for improved resilience

In response to these challenges, enterprises are adopting a range of strategies to bolster their resilience:

Embracing AI-Driven automation: Automation through AI is becoming a top priority for many enterprises as it offers proactive solutions for detecting and addressing operational risks before they cause downtime. AI-driven monitoring and self-healing systems reduce the need for human intervention during outages.

Strengthening regulatory compliance: Organizations are recognizing the need for more robust disaster recovery and compliance protocols to meet the stringent requirements of regulations like DORA and NIS2. This includes investing in secure, compliant data architectures that support data sovereignty across multiple regions.

Adopting distributed systems: Enterprises are increasingly investing in distributed systems to ensure uninterrupted service even during system failures. These systems are designed to automatically handle failures by making services available and by replicating data across multiple nodes and geographic locations, thereby shrinking the threat surface for potential service disruptions and outages.

Downtime is inevitable. To deal with this truth, these strategies highlight a forward-looking approach where technology and governance go hand in hand to secure the operational resilience of modern enterprises.

By aligning their technical estates with distributed architecture, automation, and regulatory requirements, companies can improve their uptime and their ability to adapt to an increasingly complex and regulated digital environment — while putting less stress on their technical teams and the business's bottom line.

PART 6

How distributed SQL helps organizations achieve operational resilience

Applying data and results from this report demonstrates how a distributed SQL database can help enterprises increase their organizational resilience by mitigating the technical risks and weaknesses that lead to outages.

Here are key ways distributed SQL databases help organizations improve their operational resilience and align with regulatory requirements, current or future:

Minimizing unplanned downtime: According to the survey, unplanned downtime is a major concern, with 93% of tech executives losing sleep over the financial impact of outages. Meanwhile, more than half of the financial services companies and banks (and 60% of ecommerce companies) surveyed report experiencing service interruptions weekly or even more frequently.

Planned downtime is still downtime: Beyond preventing outages, organizations dealing with frequent planned downtime due to software upgrades or application changes can recapture that uptime with the capabilities available in some distributed SQL solutions. For example, CockroachDB offers online updates and live schema changes for zero downtime of any kind in production.

Distributed SQL databases provide high availability via a fault-tolerant design and active-active replication architecture. They include disaster recovery capabilities to keep any downtime that does occur to the absolute minimum defined by an organization's RPO and RTO goals — and operational resilience regulatory requirements.

Automated failover and disaster recovery: Operational continuity — keeping systems and services available and online, even in adverse events — is a core tenet of operational resilience. Because machines can almost always react faster than humans, intelligent automation of systems is critical to optimizing resilience. Recent regulatory requirements for business continuity during system failures or cyber incidents are rooted in the fact that many current databases do not offer sophisticated capabilities for automating resilience.

Distributed SQL systems like CockroachDB automatically replicate data across geographic locations to provide continuity, even in the face of entire-region outages. If a node fails, the system automatically routes traffic to healthy nodes, ensuring continuity without manual intervention. Other cross-cluster replication capabilities can be used to achieve a low RPO/RTO depending on deployment topology and latency requirements.

Data integrity and compliance: Data integrity is a second core tenet of operational resilience — and 36% of executives in this survey say they worry about outage-related data loss and corruption. Distributed databases allow enterprises to maintain control over where specific data resides, helping to meet the data residency requirements of data privacy laws such as GDPR while also optimizing availability. For instance, CockroachDB supports features that enforce data sovereignty by keeping specific data in servers located in different geographic locations while simultaneously enabling high availability across regions. In addition, CockroachDB supports data encryption in flight and at rest to enhance security, and Auth-Z/N mechanisms to designate who can get access to what information.

Faster recovery times: The survey notes that 57% of organizations are only moderately organized in their response to unplanned downtime and meeting their RPO/RTO goals. Distributed SQL databases offer built-in mechanisms for faster recovery times, and the most mature ones, like CockroachDB, fully automate these mechanisms. These capabilities align with DORA's requirement for prompt incident management and recovery protocols

By minimizing downtime, enabling quick recovery, assisting with compliance with data residency laws, and enhancing overall operational resilience, distributed systems and SQL databases can help enterprises meet DORA requirements — and help the 79% of executives who admit their organizations risk punitive fines and other penalties because they are simply not prepared to comply with operational resilience regulations.

CockroachDB

cockroachlabs.com