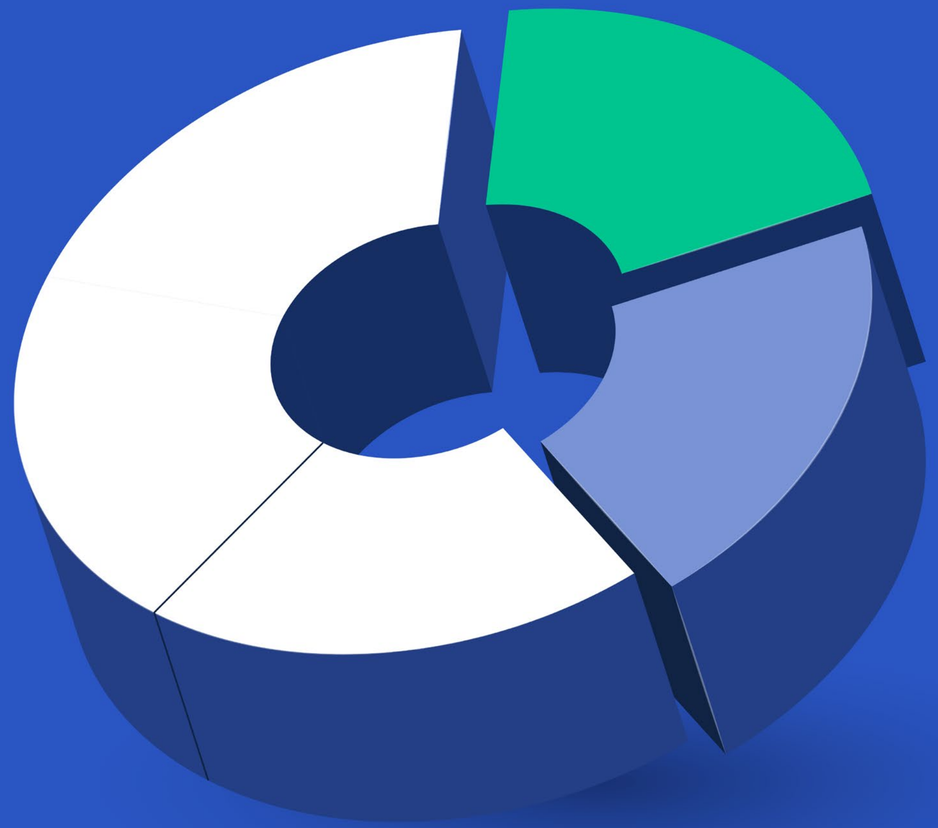
Third annual IT disaster and cyber recovery report

In 2025, enterprises are navigating a perfect storm as AI redefines cyber and IT disaster recovery



cutover

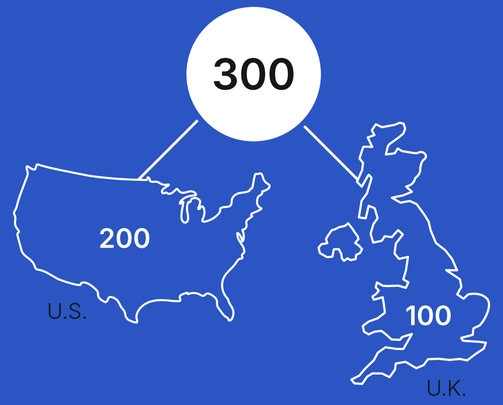
Organizations are struggling with a concerning trend: increasing IT disruptions coupled with slower recovery times, particularly evident in cybersecurity, where **77% report slower cyber attack recovery year-over-year.**

TABLE OF CONTENTS

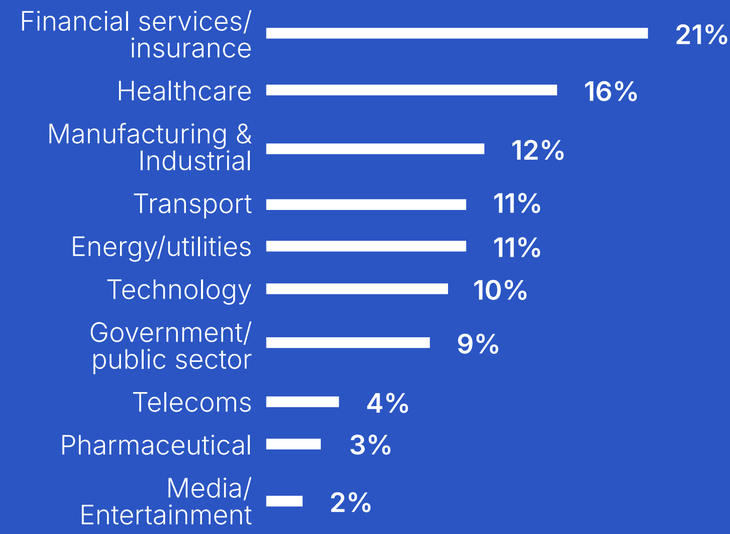
About this report

The “Third annual IT disaster and cyber recovery trends and insights report” is written by Cutover, supported by Insight Avenue. The report’s findings are based on a survey of IT decision makers and influencers at major corporations, conducted in March and April of 2025. The 300 respondents represent 10 sectors (financial services, technology, manufacturing, healthcare, transportation, energy, public sector, telecommunications, pharmaceuticals, and media) and two countries (the U.S. and the U.K.). Nearly half are Director level or C-level, with the remainder working as senior managers or disaster recovery specialists. Approximately one-quarter work in enterprises with 10,000 or more employees, while the remainder work in mid-sized (1,000-4,999 employees) to large (5,000-9,999 employees) businesses. The report supplements the survey findings with secondary research. Cutover would like to thank the participants for their time and insights.

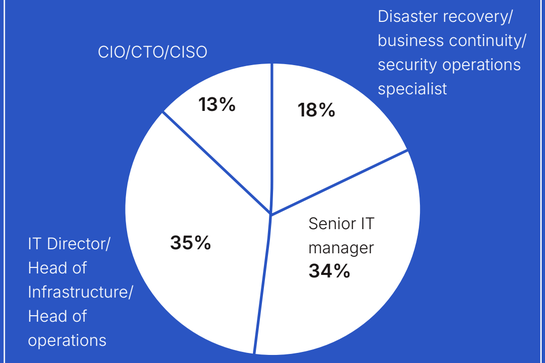
RESPONDENTS



INDUSTRY SECTOR



JOB FUNCTION / ROLE



NUMBER OF EMPLOYEES

Executive summary

Organizations are grappling with a critical and growing gap in IT resilience, characterized by increasing disruptions and slower recovery times, largely due to outdated disaster recovery plans and a persistent reliance on manual processes. This exposes enterprises to significant systemic risks, including regulatory penalties and financial losses, as many fail to meet crucial Recovery Time Objectives (RTOs) for mission-critical applications. However, the anticipated integration of agentic AI and automation promises to revolutionize disaster recovery, offering a clear path to enhanced resilience and a significant competitive edge.

Cutover, supported by Insight Avenue, surveyed IT executives, decision makers, and influencers located in the U.S. and U.K. Our research found the following trends and insights:

The widening resilience gap and increasing recovery times

Organizations are struggling with a concerning trend: increasing IT disruptions coupled with slower recovery times, particularly evident in cybersecurity, where 77% report slower cyber attack recovery year-over-year. This slowdown stems from outdated disaster recovery plans that fail to keep pace with evolving threats, with most enterprises not regularly updating their strategies. The persistent reliance on manual processes introduces significant human error and operational vulnerabilities, directly contributing to delayed recoveries. Consequently, over two-thirds of enterprises view regulatory penalties and the inability to recover from cyber attacks as major risks due to these outdated procedures.

Cyber, cloud, and regulation: A perfect storm

Organizations face a growing challenge from rising cloud outages and cyber threats, yet nearly half still struggle to adapt traditional disaster recovery strategies to the cloud's unique demands, creating a critical resilience gap. This vulnerability is increasingly addressed by new regulations like Digital Operational Resilience Act (DORA), which act as catalysts for significant DR improvements. These mandates compel organizations to enhance operational resilience, particularly concerning risks from third-party IT providers, forcing them to fortify DR capabilities against external dependencies and ensure rapid recovery from disruptions.

The RTO reality check: A systemic risk

Many organizations are failing to meet mission-critical Recovery Time Objectives (RTOs) for their most vital applications, with only a 64% success rate, leaving organizations exposed in over one-third of incidents.. This introduces significant systemic risks, including severe reputational damage, substantial financial loss, and widespread operational disruption. Clearly, there's an urgent need for more robust, well-tested, and highly visible IT resilience strategies.

Disaster recovery automation: The next differentiator

AI is set to revolutionize disaster recovery (DR), with nearly all organizations anticipating its impact within the next few years. There's significant excitement for agentic AI, as most expect it to transform both the design and execution of DR plans through automated decision-making, rapid root cause analysis, and self-healing capabilities. While challenges like skill gaps and compliance remain, early AI adoption in DR promises a substantial competitive advantage.

Agentic AI: Game changer on the horizon

AI is poised to fundamentally transform disaster recovery (DR), with nearly all organizations anticipating its impact within the next two to three years and strong enthusiasm for the opportunities it presents. Agentic AI is expected to revolutionize both the design and execution of DR plans, enabling automated decision-making, rapid root cause analysis, and even self-healing systems. Despite this immense potential, challenges like the need for specialized skills, vendor readiness, and compliance issues must be overcome for widespread adoption. Ultimately, early adopters of AI in DR stand to gain a significant competitive advantage in the market.

Inaction's High Cost: The Growing Risks to IT Resilience

Many organizations are dangerously unprepared for IT disruptions, with a concerning 31% failing to update their disaster recovery (DR) plans in over a year. This widespread inaction leaves enterprises vulnerable to severe consequences, including significant regulatory penalties, the inability to recover from devastating cyber attacks, and irreversible reputational damage.

As 2025 approaches, it's critical for businesses to act decisively, addressing both outdated strategies and persistent reliance on manual processes that hinder effective recovery. A positive shift is underway; however, with over 40% of enterprises planning to automate manual DR tasks and post-event reporting within the next two years, a proactive step towards building essential resilience.

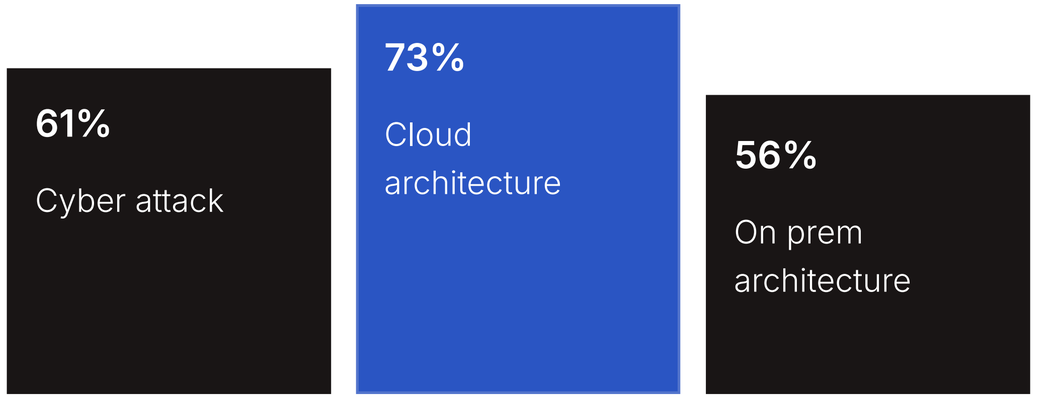
Introduction

For enterprises today, maintaining smooth IT operations is becoming increasingly challenging, primarily because of a widening gap in system resilience. Our survey reveals a concerning trend: IT disruptions and outages are escalating, and the recovery time for these incidents is simultaneously lengthening. This struggle is acutely felt in cybersecurity, with a significant 77% of organizations reporting slower cyber attack recovery than last year. This critical slowdown is no accident; it stems directly from stagnating disaster recovery (DR) plans unable to keep pace with an accelerating threat landscape.

This escalating challenge is underscored by the fact that most technology executives have experienced some degree of IT-related business disruption recently. The consequences of this widening resilience gap are severe and systemic, as organizations struggle to meet crucial Recovery Time Objectives for their most vital applications. This widespread failure leads to significant reputational damage, financial loss, and widespread operational disruption, highlighting a critical need for more robust DR strategies despite existing automation efforts.

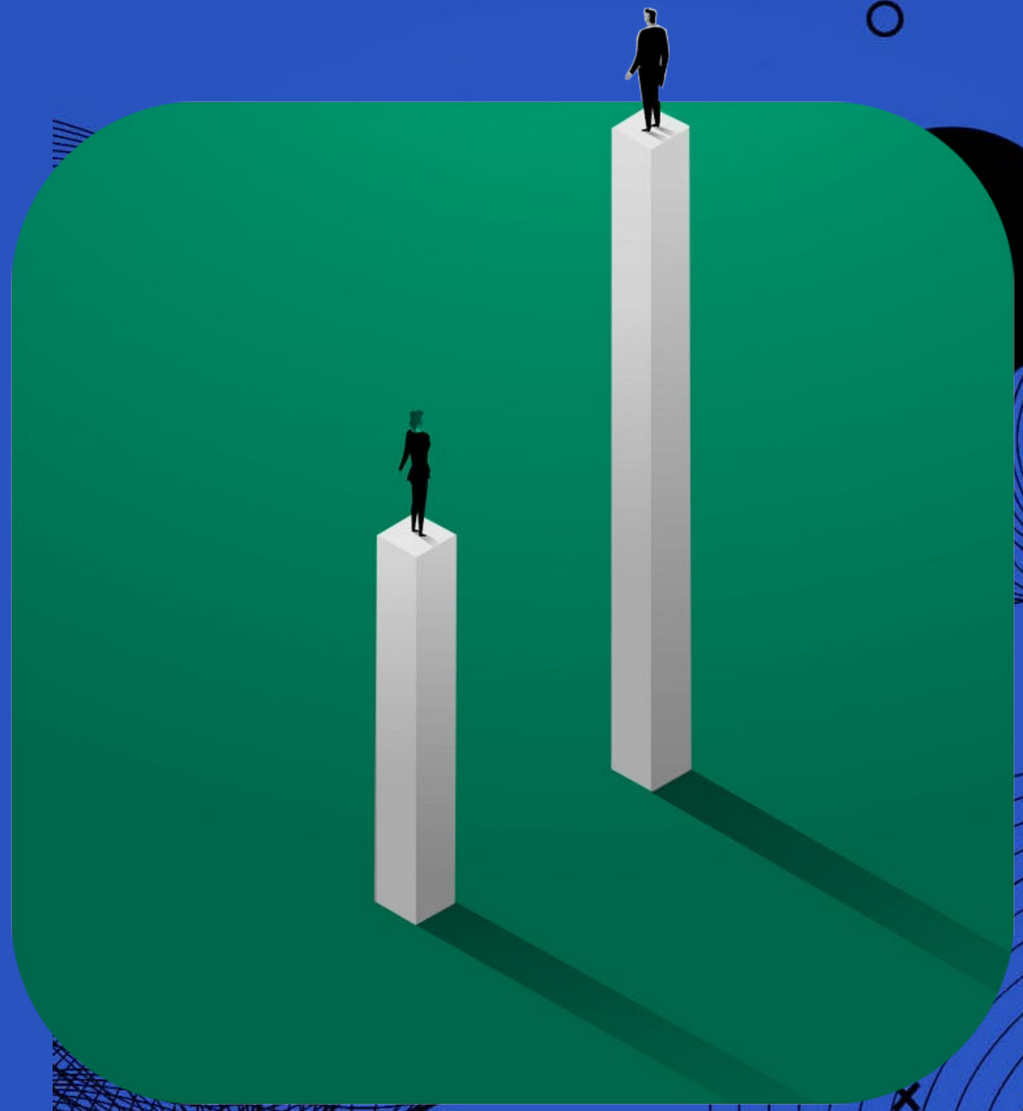
This report delves into these critical challenges, but also illuminates a clear path forward. There is growing momentum towards automating manual DR tasks and post-event reporting, complemented by the transformative potential of Agentic AI. These advancements represent not just a solution to current vulnerabilities but a strategic imperative for building truly resilient operations, driving efficiency, and securing a competitive advantage in tomorrow's digital landscape.

Has your organization experienced an increase in the following kinds of service disruptions / outages in the last 12 months?



Q1d. Has your organization experienced an increase in the following kinds of service disruptions / outages in the last 12 months?

The Widening Resilience Gap



Many organizations are facing a critical challenge: persistent IT disruptions paired with slower recovery times. The survey findings indicate a concerning trend where, year-over-year, disruption levels continue to rise while the time it takes to recover from these incidents increases. This is particularly evident in the realm of cybersecurity, where a significant 77% of organizations report that their cyber attack recovery is slower than it was last year.

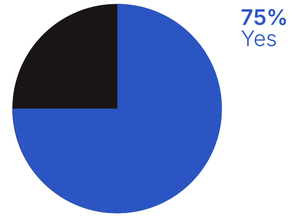
This slowdown isn't happening in a vacuum; it's often a direct result of stagnating plans failing to keep pace with accelerating threats. Despite the rapid evolution of cyber risks and other disruptive events, many disaster recovery strategies remain outdated, leaving businesses vulnerable. Only 20% of enterprises are constantly reviewing and updating DR plans, while 31% haven't updated their plans in more than 12 months. Compounding this issue is the persistent human factor and operational vulnerability, as a continued reliance on manual processes introduces significant risk and contributes to the overall slowdown in recovery efforts. Approximately two-thirds, or 64%, of enterprises view compliance and regulatory penalties and inability to recover from cyber attacks as the top two risks of outdated DR procedures.

69% say cyber attacks take longer to fully recover from now

The biggest risks to your organization of outdated disaster recovery procedures:

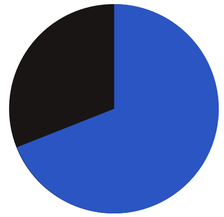
- Compliance / regulatory penalties [64%]
- Inability to recover from cyber attacks [63%]
- Reputational damage [52%]
- Loss of revenue due to customer churn [46%]
- Unnecessary pressure and stress for the IT team [39%]
- Ongoing and intensifying problems due to continued failures [35%]

Technology outages take longer to fully recover from now



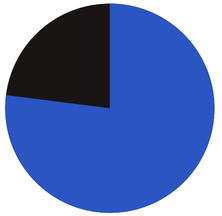
75% Yes

Cloud architecture



69% Yes

Cyber attack



77% Yes

On-prem architecture

Q4d. Do you think technology outages of the following types are taking longer to fully recover from than 12 months ago?

Q9d. What are the top three biggest risks to your organization of outdated disaster recovery procedures? TOP THREE

Cyber, cloud, and regulation: A perfect storm

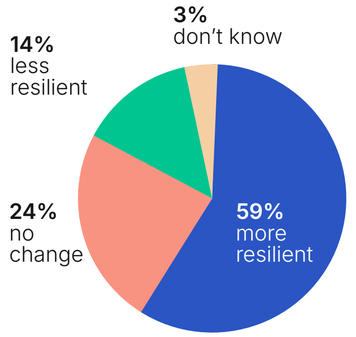
Organizations are grappling with the growing challenge of rising cloud outages and cyber threats, experiencing an increasing frequency and impact from these disruptive events. While 89% of leaders acknowledge disaster recovery as a key focus for their cloud environments, a significant hurdle remains: 48% still struggle to adapt their traditional on-premises disaster recovery strategies to the unique demands of cloud environments. This creates a critical gap, leaving many vulnerable despite recognizing the importance of cloud resilience.

This deficit is further compounded by a "perfect storm" of escalating cyber threats, the complexities of cloud adoption, and mounting regulatory pressure. New mandates, such as DORA, are increasingly serving as powerful catalysts. These regulations compel organizations to enhance operational resilience, particularly in addressing risks associated with third-party information and communication technology (ICT) providers, thereby forcing a critical re-evaluation and fortification of DR capabilities against external dependencies.

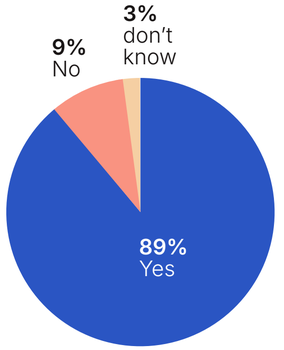
89%

of leaders acknowledge disaster recovery as a key focus for their cloud environments

Do you think operating on the cloud makes you more or less resilient?



Is disaster recovery a key focus when operating in the cloud?



Q5a. Do you think operating on the cloud makes you more or less resilient? Select one
Q5b. Is disaster recovery a key focus when operating in the cloud? Select one

Impact of increasing regulation on resilience and disaster recovery processes

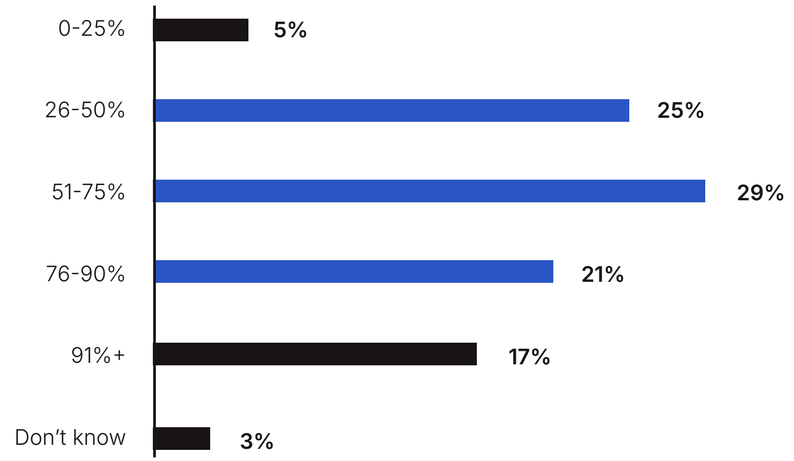
Regulatory Catalysts: The role of new regulations (e.g., DORA) in driving DR process improvements, especially concerning third-party ICT. **57%** of financial institutions are including ICT third parties in DR testing for DORA law.

Q6a. How are industry regulations impacting your resilience and disaster recovery processes? Select all that apply

The RTO reality check: A systemic risk

Despite best efforts, many organizations face alarming mission-critical RTOs, with a concerning statistic revealing only a 64% success rate for their most vital applications. The consequences of this failure are severe, introducing systemic risks to recover within their designated timeframe. This directly impacts the business, leading to significant reputational damage, substantial financial loss, and widespread operational disruption, underscoring the urgent need for more robust and reliable recovery strategies. There's an urgent need for robust, well-tested, and highly visible IT resilience strategies.

Success rate in meeting predefined RTO for mission critical applications



Q11. What is your success rate in meeting your predefined Recovery Time Objective (RTO) for mission-critical applications? Select one

Automating DR: From necessity to competitive edge

Despite clear evidence of its benefits, disaster recovery (DR) automation faces a perplexing paradox: 85% of organizations report that their investment in automation has improved DR, yet 80% also state that their DR processes need to be more automated within the next 12 months to avoid serious consequences. This highlights a critical gap between recognizing the value of automation and its widespread adoption.

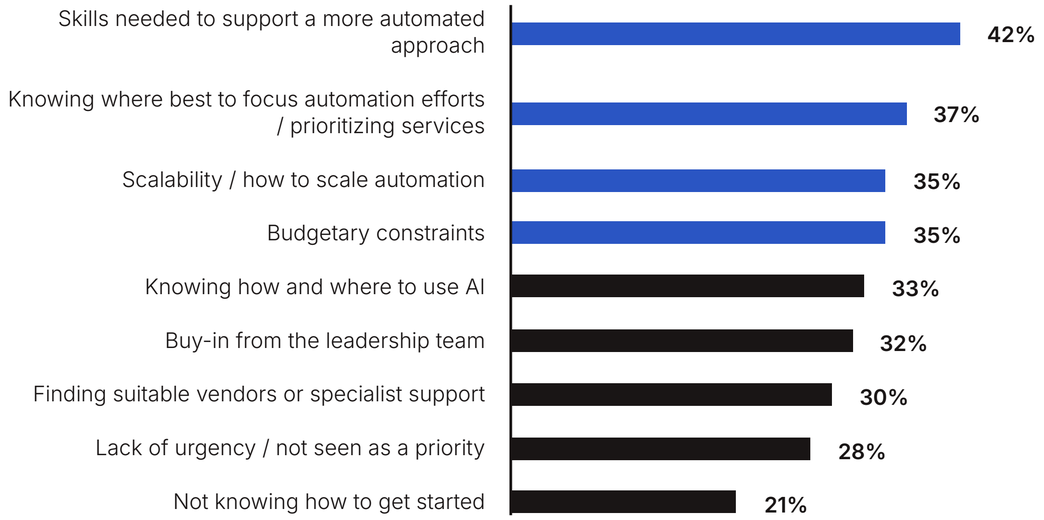
Achieving best-in-class DR automation hinges on two crucial characteristics: continuous awareness and real-time monitoring, coupled with improved visibility and control of recovery processes. These elements enable organizations to proactively manage their resilience. However, barriers often hinder progress, including persistent skills gaps, concerns over the initial investment, and simply knowing where to begin the automation journey.

85%

say automation investment has improved their disaster recovery, yet most aren't automating widely today

Overcoming these challenges unlocks what we call "profitable resilience." DR automation not only strengthens an organization's ability to withstand and recover from disruptions but also drives significant cost efficiencies. In fact, the top three benefits cited for DR automation are improved efficiency and profitability, enhanced IT staff productivity, and ultimately, reduced recovery costs. Embracing automation isn't just about avoiding consequences; it's about building a more robust and financially sound operational foundation.

Barriers or objections to automating disaster recovery

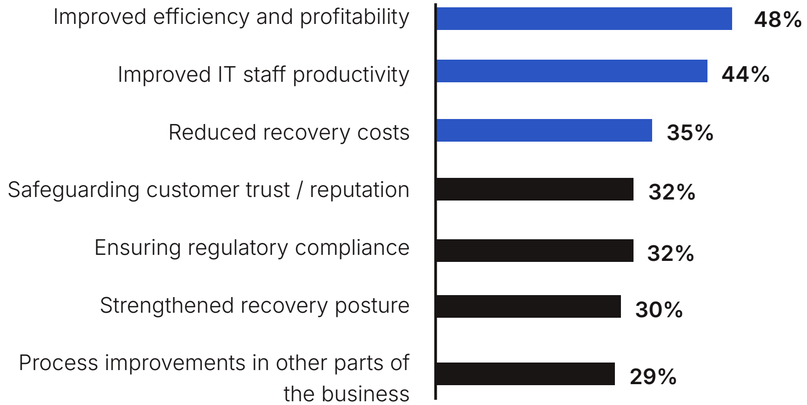


Q17a. What do you see as the barriers or objections to automating disaster recovery in your organization? Select all that apply

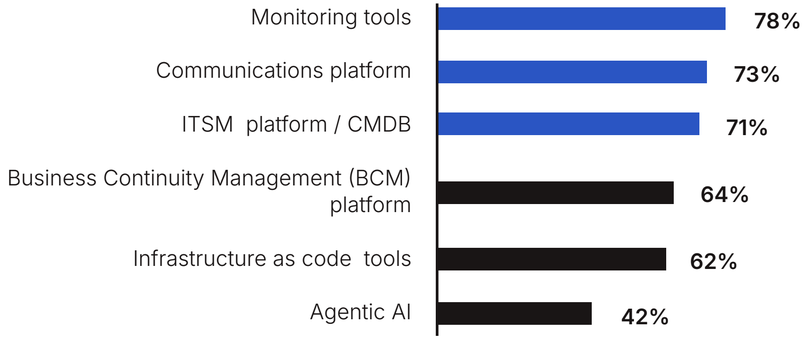
On the positive side, many enterprises are already reaping the benefits of DR automation. 55% already automate with other systems in the tech stack and automate manual, repetitive tasks. Furthermore, the use of technology tools during a live DR or testing scenario has increased (year over year) in all categories. Most notable increases year over year include:

- 14 percentage points for communications platform points year-over-year
- 10 percentage points for monitoring tools
- 17 percentage points for Infrastructure as code tools

Biggest benefits to an organization by incorporating automation into its disaster recovery procedures



Technology tools used during a live disaster recovery or testing scenario



Q19. What do you think are the three biggest benefits an organization like yours has to gain by incorporating automation into its disaster recovery procedures?

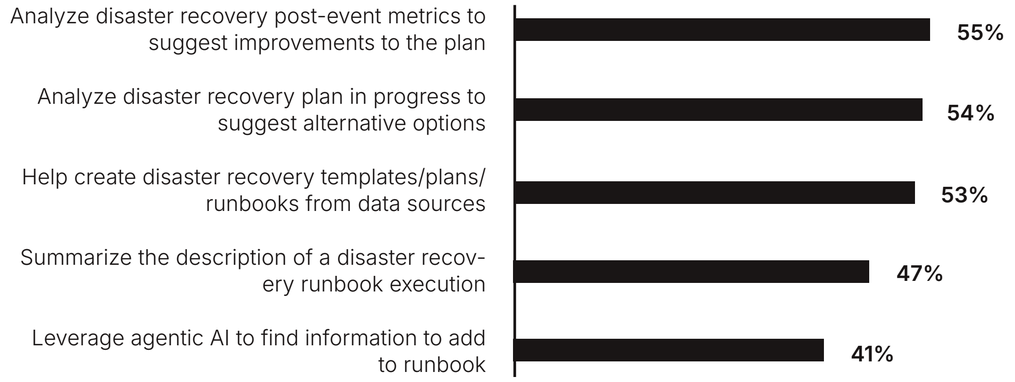
Agentic AI: Game changer on the horizon

The advent of artificial intelligence (AI) is poised to revolutionize disaster recovery (DR) processes, with a striking 98% of organizations anticipating AI's impact within the next two to three years. There's a palpable excitement surrounding this shift, as 81% of respondents express enthusiasm for the opportunities that agentic AI will bring to DR. This optimism is well-founded, given that 83% believe AI will transform the design of DR plans, and 84% foresee AI reshaping the very execution of these plans.

Agentic AI is emerging as a characteristic of best–in-class disaster recovery automation

The true potential of agentic AI in DR lies in its capacity for automated decision-making, significantly enhancing the ability to perform rapid root cause analysis and even enabling systems to become self-healing.

Ways AI is expected to impact DR processes in the next 2-3 years

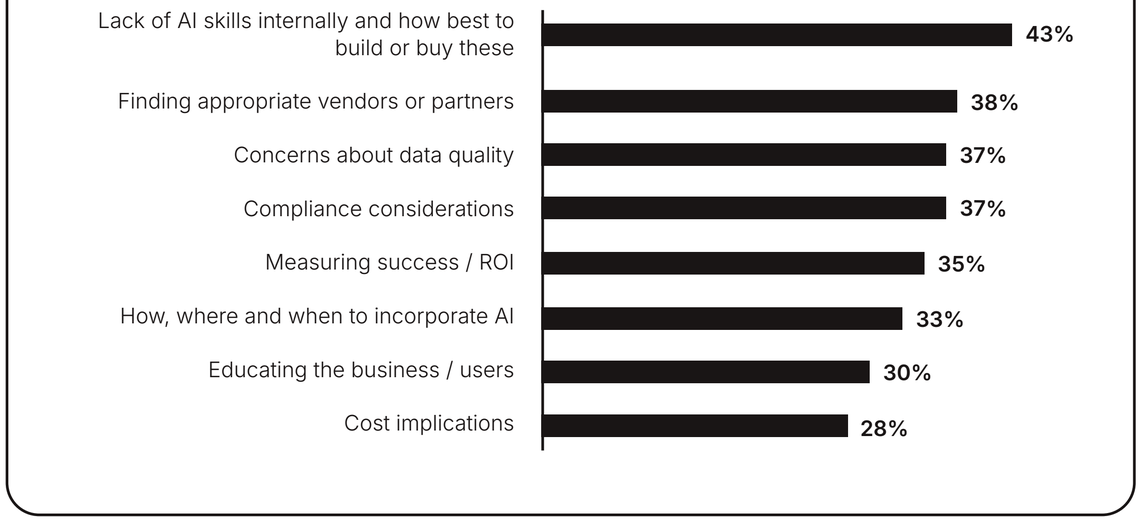


Q12. In what ways do you expect AI will impact disaster recovery processes in the next 2-3 years? Select all that apply

Agentic AI refers to autonomous AI systems that can make decisions, plan, and execute multi-step tasks with limited human oversight.

However, despite these promising advancements, key adoption blockers persist, including the critical need for specialized skills, confidence in vendor readiness, and navigating complex compliance challenges. Ultimately, organizations that become early AI adopters in DR stand to gain a significant competitive advantage, differentiating themselves as leaders while others lag behind.

Concerns around incorporating AI into DR processes



Q13a. What are your concerns about incorporating AI into disaster recovery processes in your organization? Select all that apply

Inaction’s High Cost: The Growing Risks to IT Resilience

Many organizations are playing a dangerous game with their disaster recovery (DR) strategies. A concerning 31% haven't updated their DR plans in 12 months or more, leaving them highly vulnerable. The risks of this inaction are severe and well-documented, including hefty regulatory penalties, the potential inability to recover from debilitating cyber attacks, and irreversible reputational damage.

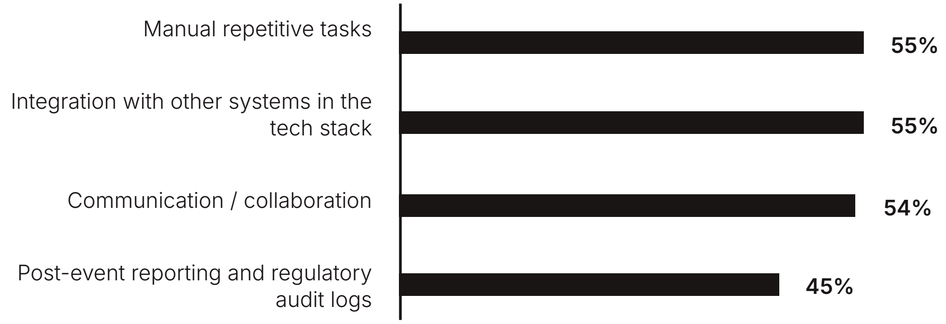
31%

haven't updated DR plans in 12+ months

2025 represents a critical deadline for organizations to act decisively before they face forced compliance or significant disruption. This inertia isn't always due to negligence; it can stem from overconfidence in existing systems or a misjudgment of current technological resilience. While some enterprises have shown maturity in incorporating automation into their DR processes compared to last year, a substantial 27% still operate with unstructured DR, lacking documented plans or relying on siloed testing and execution. Clearly, there's still significant work to be done across the board.

Looking ahead, the shift towards automation is gaining momentum. Over the next 12 months, 29% of enterprises plan to automate manual, repetitive tasks within their DR processes, and 38% intend to automate post-event reporting and regulatory audit logs. This proactive approach will be essential for building the resilient operations needed to navigate today's complex threat landscape.

Which elements of disaster recovery have you already automated or do you plan to automate



Q15e. Which elements of disaster recovery have you already automated or do you plan to automate?

Summary

Bridging the resilience gap with proactive automation

This year's findings paint a clear picture: enterprise IT resilience is at a crossroads. We're seeing more outages, from escalating cyber attacks—with 77% of organizations reporting slower recovery—to increasing cloud outages. Yet, recovery times are lengthening, often due to outdated disaster recovery (DR) plans, many left untouched for over a year, and an over-reliance on error-prone manual processes. The consequences are dire, impacting everything from financial stability to reputation and regulatory compliance, as evidenced by a mere 64% success rate for mission-critical RTOs.

The imperative for change is intensified by rising threats and new regulations like DORA, demanding stronger operational resilience, especially concerning third-party dependencies. While leaders acknowledge the importance of cloud DR, nearly half still struggle to bridge the gap from traditional strategies to cloud environments, underscoring the urgent need for comprehensive, well-tested, and highly visible resilience strategies.

Despite a paradox where 85% recognize DR automation's benefits but 80% still need more of it, a crucial shift is underway. With significant planned automation of manual DR tasks and post-event reporting in the next year, coupled with the transformative potential of Agentic AI, which 98% of organizations anticipate impacting DR—the path to a truly resilient future is becoming clear. Integrating automation and AI isn't just about avoiding risk; it's a strategic imperative that enables proactive recovery, drives efficiency, and ensures businesses can not only withstand inevitable disruptions but also emerge stronger, seizing a distinct competitive advantage.

cutover

Cutover provides enterprise technology operations teams with an AI-powered SaaS solution that automates and streamlines complex processes with intelligent runbooks. The Cutover solution enables teams to quickly respond to incidents, recover from IT outages, and manage cloud migrations with precision and efficiency. Cutover is used in many of the world's largest financial institutions to support their critical technology operations including 5 out of the top 6 largest asset managers and 3 out of the out of the top 5 US banks.

cutover

Automated runbooks for technology teams

Learn about how **Cutover's AI-powered runbooks** help enterprises reduce mean time to resolution, **recover 50% faster,** and unlock the strategic advantages of true automation.

Visit www.cutover.com.