cutover

The IT disaster and cyber recovery trends and insights report

In 2023, 75% of organizations experienced IT service outages, recognize the need to increase investment in cyber disaster recovery and want to automate disaster recovery in the next 12 months

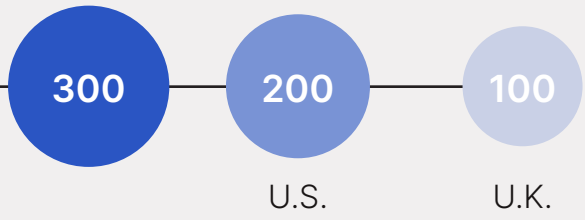
Table of contents

About this report

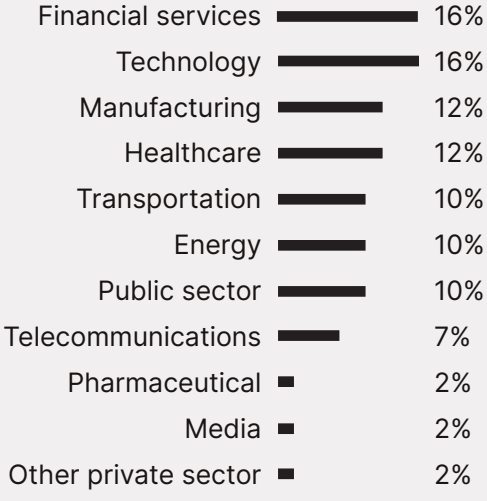
"The IT disaster and cyber recovery trends and insights" is a report written by Cutover, supported by Insight Avenue. The report's findings are rooted in a survey of IT decision-makers and influencers at major corporations, conducted in July 2023.

The survey

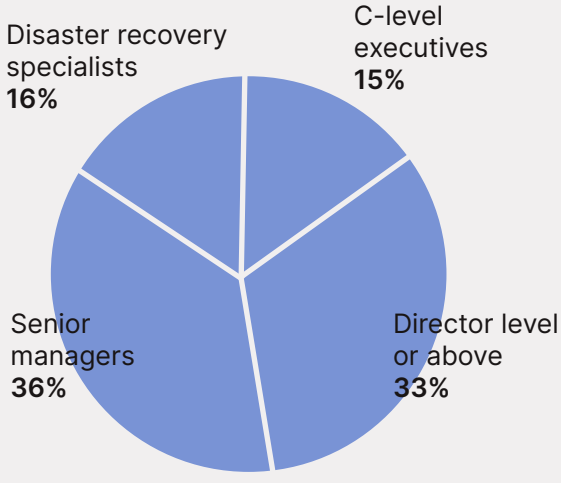
RESPONDENTS



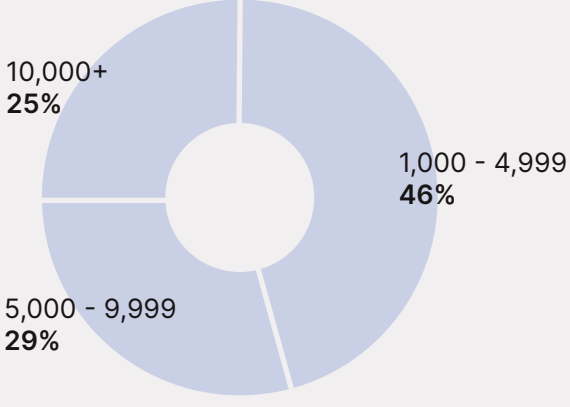
INDUSTRY SECTOR



JOB ROLE / FUNCTION



NUMBER OF EMPLOYEES



The report supplements the survey findings with secondary research. Cutover would like to thank participants for their time and insights.

Executive Summary

Most enterprises have experienced some degree of IT-related business disruption in the last 12 months. While most organizations are taking advantage of the benefits of cloud hosting, this doesn't necessarily correlate to less disruption. In fact, our research shows that enterprises face an increase in service disruption related to cloud architecture as well as cyber attacks. Cutover, supported by Insight Avenue, conducted a survey of IT executives, decision makers and influencers located in the U.S. and U.K.

Our research found that:

Outdated disaster recovery plans cause significant business risk

Most enterprises (75%) have seen significant risks associated with outdated disaster recovery (DR) procedures, nearly one-third (31%) aren't keeping their DR plans updated.

Cybersecurity is top of mind and concern is increasing

More than four in five respondents (85%) stated cyber disaster recovery is a priority and they know their organization must invest more here. Moreover, nearly all enterprises agree (94%) there is concern about recovering from different technology disaster scenarios such as cyber attacks.

There is a need for more automation

Most enterprise respondents (72%) note that DR needs to be more automated within the next 12 months to avoid serious service disruption and any associated reputational and financial consequences. Respondents predict varying gains from automating DR processes, including improved efficiency and profitability (47%), improved IT staff productivity (47%) and enhanced customer trust and retention (45%).

The IT disaster recovery revolution is here

Enterprises are dealing with an increase in IT service disruptions coupled with recovery times that are longer than 1-2 years ago. While digital transformation initiatives have expedited, DR procedures have not kept pace.

Introduction

The pressure is on for enterprises to keep pace with the rapidly changing economy and landscape. In the first half of 2023, global growth slowed while inflation and interest rates skyrocket and geopolitical instability increased. At a more micro level, IT teams are at the tipping point of disruption - they are strained, with limited resources, and are dealing with mixed skillsets and increasing backlogs.[1] This holds true across most IT specialties including IT DR and cyber recovery.

The shift to public cloud infrastructure has compounded complexity, particularly for IT and cyber disaster recovery. However, this shift has not decreased IT-related business disruption. In reality, organizations are experiencing outages and struggling to fully recover more now than ever, and human error plays a major role. Uptime Institute reports that more than 70% of data center outages are caused by human error.

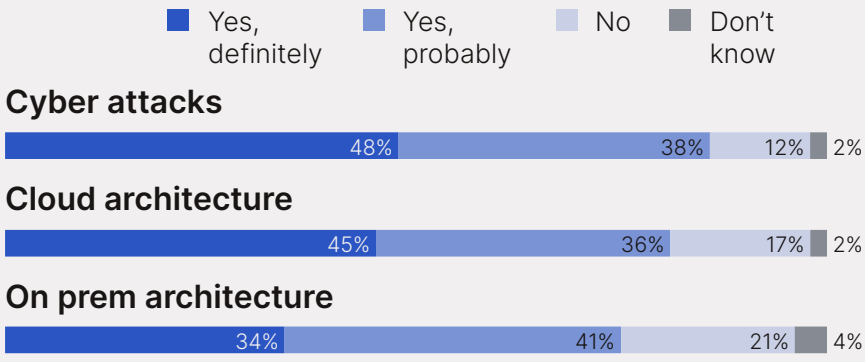
In a survey of U.S. and U.K. technology executives, 75% of respondents said they have experienced some degree of IT-related business disruption in the last 12 months. The increase in IT service disruptions and outages is correlated to cloud architecture and cyber attacks and to a lesser degree on-premises architecture. Most IT executives expressed concern about recovering from different technology scenarios including cyber attacks, software failure, network outages and more.

> 75% of IT executives say they have experienced some degree of IT-related business disruption in the last 12 months

Furthermore, technology outages are considered to take longer to fully recover from now than 1-2 years ago, particularly cyber attacks (87%), cloud architecture outages (81%), and on-premises architecture (75%). More respondents in the financial services sector (96%) say outages take longer to fully recover from than they did 1-2 years ago, compared to other industry sectors (85%).

Technology outages are considered to take longer to fully recover from now than 1-2 years ago – particularly cyber attacks (87%), outages with cloud architecture (81%) as well as on prem architecture (75%)

Belief that technology outages take longer to fully recover from now than 1-2 years ago



Technology outages are considered to take longer to fully recover from now than 1-2 years ago – particularly cyber attacks (87%), outages with cloud architecture (81%) as well as on prem architecture (75%)

Outdated disaster recovery plans cause significant business risk

75% of respondents say there are significant risks to their business associated with outdated DR procedures.

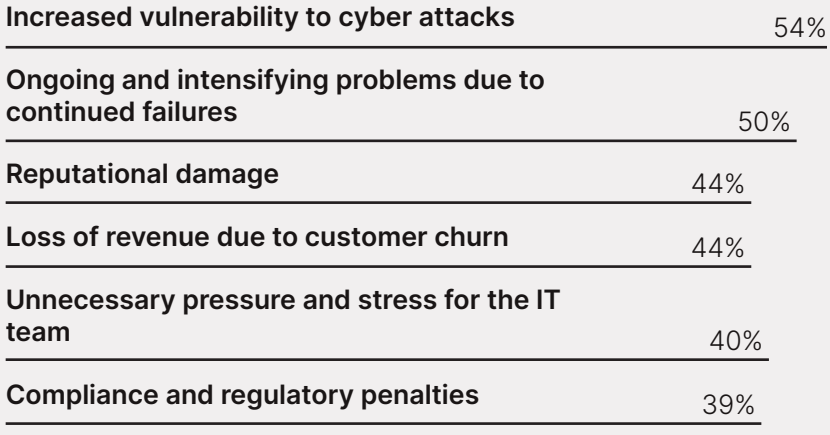
With increasing pressures on IT teams and an increase in IT service outages, many enterprises haven't evaluated or updated their DR procedures. In fact, only 15% of respondents are constantly reviewing and updating DR plans and 31% of enterprises haven't evaluated or updated their DR plans in the last year or more. While not surprising, outdated IT DR procedures cause significant risks that can negatively impact employees, customer service and reputation, and overall business health.

Similarly, a study by Veeam[2] shows that more than half (58%) of all data backups fail. This creates significant issues for enterprises experiencing cyber attacks and outages. Testing backup solutions and full recovery scenarios can help avoid these negative outcomes, but if recovery procedures are outdated, risks compound.

Respondents state the biggest risks to the organization from outdated DR procedures include:

- Increased vulnerability to cyber attacks (54%)
- Ongoing and intensifying problems due to continued failures (50%)
- Reputational damage (44%)
- Loss of revenue due to customer churn (44%)
- Unnecessary pressure and stress for the IT team (40%)
- Compliance and regulatory penalties (39%)

the biggest risks to the organization from outdated DR procedures



Cloud disaster recovery proves complex

This research shows that two-thirds of enterprises struggle to adapt DR plans from their on-premises environments to the cloud. While this may sound surprising, DR complexity compounds in the cloud. Applications need to be organized by tiers and are often distributed via microservices. Then, plans need to be organized by the defined application tiers to ensure appropriate recovery time objectives are outlined.

In particular, U.S. enterprises struggle more to adapt DR plans from on-premises to the cloud - 71% of U.S. vs. 51% of UK enterprises.

Cybersecurity is top of mind and concern is increasing

> 85% say cyber disaster recovery is a priority and they know they must invest more here

It's no surprise that cybersecurity concern is on the rise. It's predicted that by 2025 cybercrime will cost the world economy approximately $10.5 trillion annually.[3] Cybercrime is increasing in professionalism resulting in sophisticated threats that strive to bypass even the most advanced cybersecurity solutions. Artificial intelligence (AI) will also play a role in powering cyber attacks with smart malware, mutating threats, and realistic phishing emails that can circumvent even the latest security protocols.

Our research shows that most enterprises (73%) say cyber outages are slowing down digital transformation progress and, as a result, they are prioritizing investment in cyber disaster recovery (85%). Nearly all enterprises agree (94%) there is concern about recovering from different technology disaster scenarios, especially cyber attacks.

More than half of respondents (56%) cite cyber threats as a major contributing factor to technology service disruptions and recognize a need for improved resilience against cyber threats. Over the next 12 months, while cyber attack vectors morph and increase in sophistication, enterprises are most concerned about ransomware (81%), but concern is distributed amongst all cybersecurity threats.

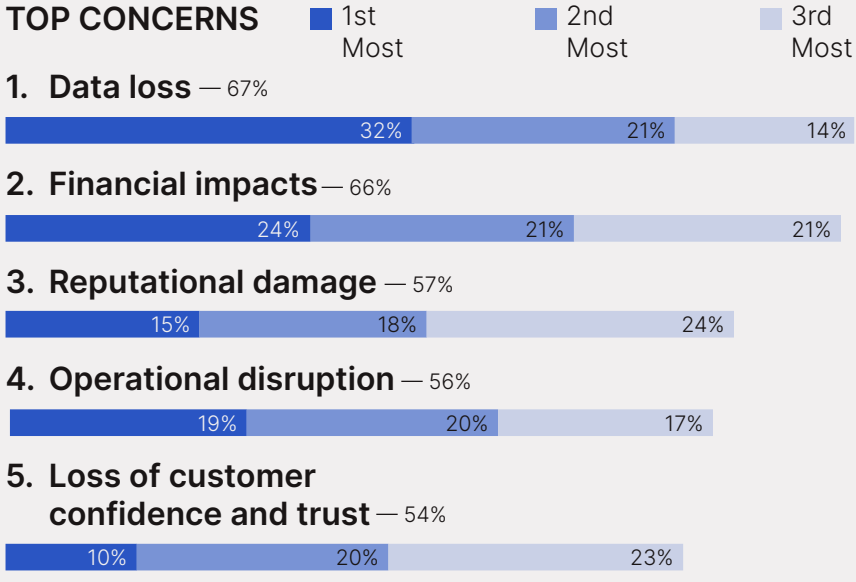
Level of concern about cybersecurity threats over next 12 months

Ransomware	81%
Viruses and malware	81%
Software vulnerabilities	79%
Cloud services security gaps	77%
DDoS	70%
Supply chain attacks	68%
Insider threats	64%

Implications of a cyber attack

With evolving and increasing cyber attacks, enterprises are concerned about various implications. Respondents cite data loss as the biggest concern (67%) followed by financial impacts (66%) and reputational damage (57%). In the U.S., the average duration of downtime after a ransomware attack is nearly three weeks. Similarly, the average downtime for a UK company experiencing a ransomware attack is 1-3 weeks.

Relative level of concern about implications of a cyber attack



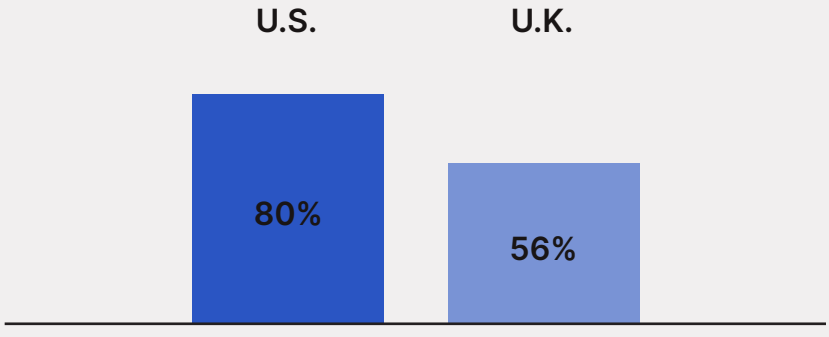
The age of automation for IT and cyber disaster recovery is here

85% agree that the best performing companies in their sector will have automated disaster recovery by 2025

Businesses across a wide spectrum, both in size and sector, are investing in AI and automation tools with significant growth expected in the next few years. Automation can enhance customer service with chatbots to cloud deployment optimization and procedural and workflow advancements.

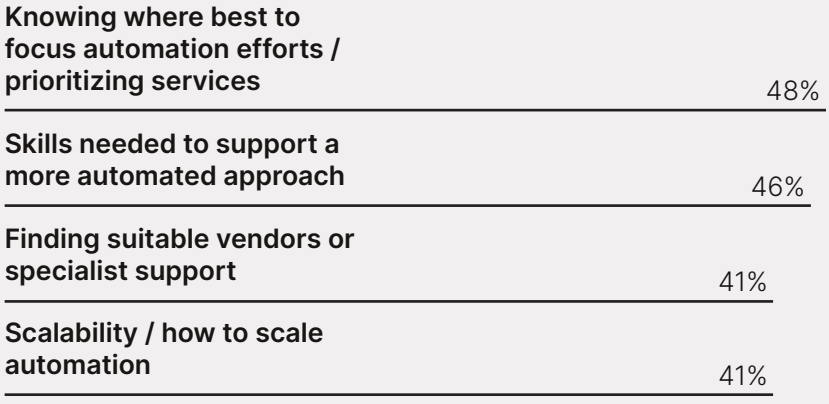
Most enterprise respondents (72%) note that DR needs to be more automated within the next 12 months to avoid serious service disruption and any associated reputational and financial consequences. More U.S. respondents think that DR needs to be more automated - 80% of U.S. vs. 56% of U.K. Comparatively, 9 out of 10 financial services institutions think DR needs to be more automated in 12 months.

U.S. respondents compared to the U.K. respondents, think DR needs to be more automated



While the majority of enterprises respond that DR needs to be more automated, it poses the question: why aren't more enterprises further along in their automation journey? Our research shows the key barriers to automating DR encompass people, technology and scalability challenges.

The key barriers to automating disaster recovery



While enterprises understand the barriers to automation, they also grasp the benefits of incorporating automation into DR processes. Respondents predict varying gains of automating DR processes include improved efficiency and profitability (47%), improved IT staff productivity (47%) and enhanced customer trust and retention (45%).

And, despite the well known benefits, most enterprises are not advanced in their DR automation maturity. **Only 14% of U.K. enterprises are advanced and the U.S. is only slightly more advanced at 21%.**

Advancement in automation reaps benefits beyond just maturity

Those with more advanced automated DR also show advancements in other key areas. They are more likely to see that migration to the cloud makes applications more resilient to cyber attacks and IT outages than those with less automation. These firms are also more likely to be evaluating and updating DR plans constantly than those with less automation.

SUMMARY

The IT disaster recovery automation revolution is here

Enterprises are dealing with an increase in IT service disruptions coupled with recovery times that are longer than they were 1-2 years ago. While digital transformation initiatives have expedited, DR procedures have not kept pace.

As cyber attacks increase in volume and sophistication, IT teams strain to cope with growing cybersecurity concerns. In fact, cyber outages are slowing down digital transformation progress and organizations are most worried about data loss, financial implications, reputational damage, operational disruption and loss of customer confidence and trust.

Firms recognize the need to increase investment in DR generally and specifically in cyber disaster recovery.

85% recognize that they need to increase investment in disaster recovery generally

About Cutover

Since 2015, Cutover has helped enterprises standardize and automate technology operations processes for IT DR, cyber recovery, release management and cloud migration to increase efficiency and reduce risk. Cutover's Collaborative Automation SaaS platform bridges the gap between teams and technology with dynamic, automated runbooks.

Sources:

1. Appian, 2021, **"IT's changing mandate in an age of disruption"**, The Economist Intelligence Unit

2. Veeam Software, 2021, **"Data Protection Report 2021"**

3. Cybersecurity Ventures, 2022, **The 2022 Official Cybercrime Report**, eSentire

Learn more about how Cutover's automated runbooks help enterprises increase efficiency and reduce risk with streamlined disaster recovery processes.

BOOK A DEMO