

## REPORT REPRINT

# With costly outages on the rise, disaster recovery is still a top issue

**AUGUST 17 2020**

**By Henry Baltazar**

In 451 Research's Voice of the Enterprise: Storage, Data Management & Disaster Recovery study, outages were common and led to costly losses. Automation and AI-enhanced management will have a major role in improving resiliency and dealing with disaster recovery challenges.

---

THIS REPORT, LICENSED TO STORAGE GUARDIAN, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR RE-POSTED, IN WHOLE OR IN PART, BY THE RECIPIENT WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.



**S&P Global** Market Intelligence

### Introduction

In 451 Research's Voice of The Enterprise (VotE): Storage, Data Management & Disaster Recovery 2020 survey, respondents answered questions about the cause of their most recent outage and the impact in terms of costs and other factors such as damaged reputation and lost customer loyalty. To deal with disaster recovery (DR) challenges, organizations are looking to leverage automation, cloud services and other new innovations to improve the resiliency of their infrastructures.

### 451 TAKE

Disaster recovery has been a top storage and infrastructure pain point for several years, and given the substantial negative impact of outages, organizations will need to continue to enhance the resiliency and recoverability of their infrastructures. DR testing and preparedness are key areas where improvement is necessary given that 20% of respondents either did not test their DR plans (14%) or simply didn't have DR plans in place (6%), according to our VotE: Storage, Budgets and Outlook 2020 survey.

Automation is another key area where organizations should focus since this will not only make it easier to test DR plans, but it will also make recovery operations faster and more consistent since human errors could be minimized. Another key cog in the disaster recovery modernization effort is public cloud storage, where elasticity has become attractive since it keeps costs down until a failover operation is necessary. This trend should continue for many organizations since few have an appetite for creating and maintaining additional datacenters and the IT infrastructure within them.

### Outages are costly, with many negative consequences

In our recent VotE: Storage, Data Management & Disaster Recovery survey, 30% of respondents reported that they had a significant outage in the past two years, and this statistic was even worse for larger organizations with over 1,000 employees, which had approximately 40% of respondents reporting an outage in the past two years.

Nearly half of these outages (49%) led to losses over \$100,000 for the affected companies. The largest organizations, which had headcounts of 10,000+ employees, had a higher proportion of costly outages, with 13% of respondents reporting an outage costing over \$1m compared with midsized (1,000-9,999 employees) companies, where 8% suffered through a \$1m+ outage.

The negative impact of lost or unrecoverable backup data can impact an organization in multiple ways (see Figure 1). Lost worker productivity was the most frequently chosen negative impact for 49% of the respondents, which emphasizes why speed of recovery is important to get those workers back on track as soon as possible with minimal data loss. Data loss and outages also impact the reputation of an organization (35% of respondents) and customer loyalty (19%), which should be a key concern for those focused on delivering a strong and consistent customer experience.

## Figure 1: DR Failures Lead to Multiple Negative Consequences

Source: 451 Research's Voice of the Enterprise: Storage, Data Management & Disaster Recovery 2020



Base: All Respondents (n=520)  
Source: 451 Research's Voice of the Enterprise: Storage, Data Management & Disaster Recovery, 2020  
Which of the following effects would your organization experience most due to lost or corrupted backup data? Please select up to two.

### A wide range of causes lead to outages

In the study, no single type of incident was responsible for the majority of recent outages, which shows that organizations need to shore up their infrastructure in multiple dimensions to reduce outage risks. Software failure was the cause of the most recent outage for 22% of respondents, with hardware failure coming in a close second at 20% (see Figure 2). Financial services respondents in particular were hit hard by software (38%) and hardware failures (30%) compared with the other industries.

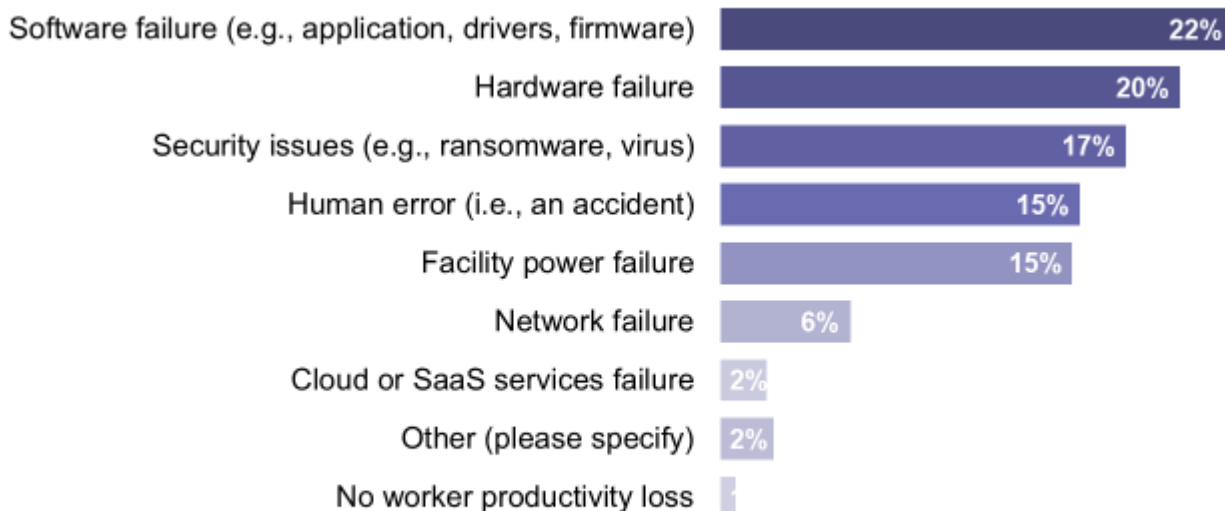
Security issues like ransomware and viruses resulted in outages for 17% of respondents, and this has been a point of emphasis for storage vendors that are looking to improve recoverability while also ensuring that an uncompromised, golden copy of data is available when the data protected in other recovery options such as snapshots and short-term backups is corrupted. Human error was a cause of failure for 15% of respondents and proponents of automation claim that the reduction of manual processes that often create these errors could substantially boost reliability and consistency.

Although facility power (15%) and network failures (6%) are often discussed as a byproduct of natural disasters such as hurricanes, in the survey these two types of failures were lower on the list compared with the previously mentioned issues. Cloud or SaaS failures were responsible for only 2% of the respondents' most recent outages, although we expect this figure to rise as a growing number of organizations leverage these services for production workloads.

## REPORT REPRINT

### Figure 2: Software, Hardware and Security Issues Were Responsible for Most Outages

Source: 451 Research's Voice of the Enterprise: Storage, Data Management & Disaster Recovery 2020



Base: Respondents who have experienced an outage resulting in lost data or productivity (n=305)

Source: 451 Research's Voice of the Enterprise: Storage, Data Management & Disaster Recovery, 2020

What was the cause of your organization's most recent downtime incident that affected worker productivity as it relates to data protection?

## Recommendations

- **Improve disaster recovery testing and preparedness.** As we discussed in a previous report on DR testing, only 17% of organizations test their DR implementations more than twice a year, with 46% of respondents settling for annual testing. Given the rapid changes that are occurring in production environments from software and hardware updates, even biannual testing of DR is not adequate to keep up with the pace of change of infrastructure and applications.
- **Invest in automation.** In the study, 80% of respondents said they would allow artificial intelligence or automated tools to initiate a failover operation. The negative impact of outages is exacerbated by the length of downtime. With automation in place, organizations can restore their production environments quickly and consistently at a secondary site or potentially in a cloud environment. Automation can also help facilitate and accelerate DR testing and validation.
- **Leverage AI-enhanced management and monitoring tools.** By using these tools, organizations will be able to locate issues before they become major outages. These tools often provide recommendations that customers can use to proactively improve their software and hardware updates and maintenance, which is important given that hardware and software failures accounted for 42% of failures (see Figure 2).
- **Implement cloud-based disaster recovery.** The replacement of DR sites was the top driver for respondents that were using public cloud storage services and was chosen by 37%, while 34% said they were using cloud as a replacement for tape for long-term storage. In the study, 39% of respondents were already deploying hybrid cloud data protection with local backups and long-term backup data being stored in a cloud environment. Cloud-based disaster recovery is attractive to organizations since it takes advantage of the elasticity of cloud and only consumes production resources when they are activated in a failover.