451 Research | Business Impact Brief

Multicloud resiliency: It's not automatic

The 451 Take

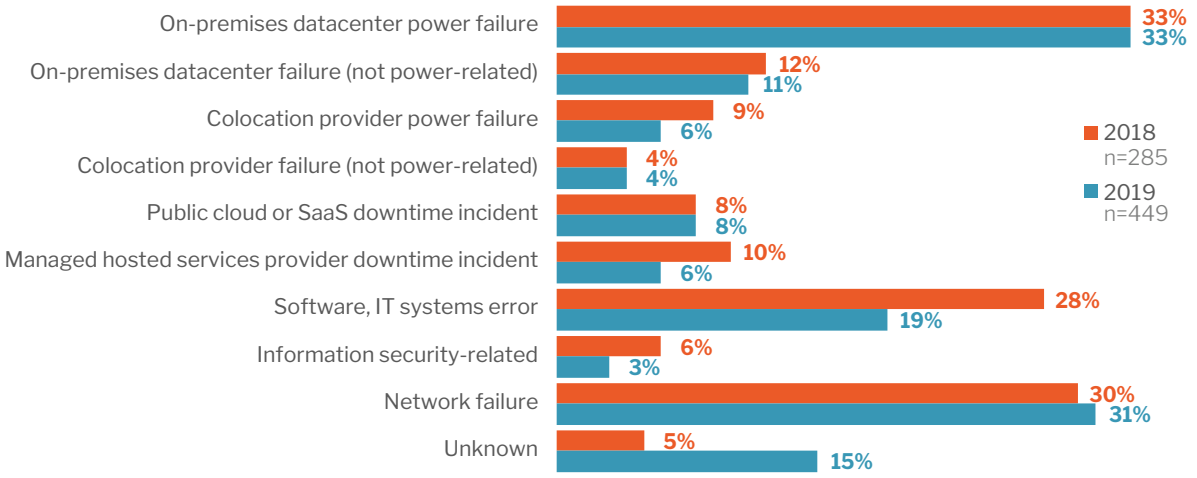
Having data in multiple places can seem like a good thing when organizations consider their situation with hybrid and multicloud deployments. However, the reality is far different. Failures occur with great regularity, and without coordinated efforts to manage the extended infrastructure and its distributed data resources, the availability of critical applications can be put at increased risk, threatening business operations. To ensure business continuity, organizations have to consider how they can recover applications and data within a tolerable time from a range of failure scenarios. The process of gaining confidence in data's security, availability and recoverability starts with understanding how data is being used across the full collection of execution environments that companies leverage and what protections make sense. While the various services offered by cloud providers can seem tempting, real application protection in a hybrid and multicloud environment is anything but automatic.

Managing risk is a complex process. Often the greatest challenge for organizations is understanding the full breadth of risks that could present themselves and how to manage them. This is especially true with the infrastructure that most organizations support today. They're in on-premises and off-premises venues with a wide variety of capabilities, use patterns and dependencies. That complexity can make it particularly difficult to understand what risks exist to applications and the data they use. Traditional business continuity and disaster recovery (BC/DR) approaches strain to scale to what hybrid and multicloud environments present. To deliver real application resiliency in hybrid, a more unified BC/DR plan is needed.

The Cause of Most Outages is Known, Yet the Frequency Remains Relatively Constant

Source: Uptime Institute Global Survey of IT and Data Center Managers 2019

Q: What was the primary cause(s) of your organization's largest or most recent outage? Select multiple causes if they apply.



An additional challenge is the state of the information security landscape. The nature of cyberattacks has continued to evolve, shifting the types of risks that they present. Attackers have moved from subverting systems and siphoning off data to adopting new strategies that use ransomware to seize data and hold it hostage, or 'wiper' malware that simply corrupts or destroys data. This new landscape requires changes in data protection to withstand these

The 451 Take (continued)

new assaults. At the same time, the decomposition of application architectures is driving the need for a more comprehensive approach to data resiliency as well. Patterns such as microservices architectures and serverless computing change how data is used and where it has to reside.

Planning for effective application protection requires organizations to understand that resiliency is a product of good design and operational effectiveness. It's a logical outcome of modern BC/DR processes. When applications and services are the fusion of various infrastructures and components in a hybrid environment, the view of what could cause an outage has to encompass the various locations, as well as the interconnections between them. That imposes much greater importance on the ability not only to protect data, but also to be able to project it to alternate locations as part of recovery efforts.

One of the greater challenges that hybrid and multicloud environments present is scale. Effective approaches for data protection have to address scale with operational simplicity. That simplicity can be driven from two critical aspects of any approach: consistent data services have to be available across heterogenous locations, and automation has to be effective to manage operational workloads.

Hybrid environments certainly present challenges, especially for security and business continuity. These environments force companies to rethink approaches that have worked in more constrained situations. The utilization of hybrid infrastructure requires that organizations move to a more comprehensive assessment of how they'll protect their core business assets. This is a shift that has to be dealt with to ensure the full resilience of such a fundamental aspect of business value.

Business Impact

ROBUST DATA AVAILABILITY. Effective planning can mitigate the additional risk that hybrid and multicloud environments bring, allowing organizations to leverage them with confidence. Business continuity in the age of hybrid requires broader coverage.

CONSISTENT DATA MANAGEMENT. Application owners benefit from consistent data services across a range of execution environments.

PROTECTION FROM CYBERATTACKS. Critical data needs to be able to withstand today's attackers' new focus on seizing or destroying data. Resiliency in the face of many challenges is critical.

FULL DATA LIFECYCLE COVERAGE. Cloud and hosting providers lack the coordinated data lifecycle management that modern businesses require. Effective protections can enable business growth while managing risk.

Looking Ahead

The future of stable infrastructure is tightly bound to the resilience of the key resources that drive it. While compute and connectivity are important, data has always been the life blood of any organization. To maintain an organization's ability to succeed and move forward in markets, its data infrastructure has to offer truly resilient access. Hybrid and multicloud environments present new challenges, but not ones that are insurmountable. With thoughtful planning, organizations can address both the challenges that the complexity of the hybrid world presents and the means to extend traditional models to meet those needs.