IT STRATEGIES FOR SEVERE WEATHER & STORMS: REDUCING DOWNTIME & DATA RISKS

Hurricanes, storms and natural disasters are a reality of life. For organizations relying on technology infrastructure to power their business, risks associated with natural disasters include IT downtime, data loss and severe interruptions in daily business operations. The challenge is most significant for organizations relying only on on-premise servers and data centers. When a natural disaster or a power outage occurs, these organizations may have limited options to regain service uptime. In fact, most solutions such as restoring the power infrastructure already lie beyond their control.

Instead of facing these risks head-on, organizations can adopt risk aversion and mitigation strategies and take advantage of cloud-based alternatives. These IT service models help organizations add redundancy into their IT systems and dynamically flow IT workloads into the most available and high performance infrastructure resources. When a server instance or data center is hit by a catastrophic storm leading to area-wide power outage, organizations can switch to data center resources in alternate geographic zones that contain the necessary data, apps and IT services to keep the business running. Meanwhile, the primary data center location can undergo restoration without impacting the business or keeping service end-user waiting. In order to ensure effective risk aversion and, the following IT strategies are useful:

Design for Resilience and Redundancy

Natural disasters are expected to have a minimal impact when organizations have the option to switch between data centers operating in disparate geographic locations. Most cloud vendors offer data center locations in regions across the nation and continents. For instance, vendors spread their cloud data center offering across isolated locations called Regions and Availability Zones. Customers can replicate their apps, services and data across different Availability Zones, each equipped with a range of fault tolerance and risk mitigation systems. A strategic approach to architecting infrastructure frameworks is required to ensure that investments in multiple isolated Availability Zones and Regions are justified and deliver adequate resilience to the IT service, apps and data assets. The designing principles should include a systematic failure recovery system such as triggering automated actions to distributed IT workloads dynamically based on continuously monitored KPIs. The resource capacity should also change dynamically to satisfy varying demand using monitoring and automation solutions offered by cloud vendors. These best practices will ensure that the infrastructure resources are always available and optimally utilized prior to and during disaster situations.

Design for High Availability

Cloud vendors typically offer Service Level Agreement (SLAs) with guarantee for a maximum limit of downtime per year. The availability limits may range from 99.9% (three nines) to 99.999% (five nines) for most customers. While both limits sound reasonable, every additional 'nine' translates into vastly different availability standard. 99.9% availability corresponds to a maximum of 8 hours and 46 minutes of downtime per year, whereas 99.999% availability corresponds to 5 minutes and 35 seconds of downtime per year. Deploying a high availability infrastructure is particularly suitable for disaster-prone geographic locations due to the risk of unplanned downtime. If this risk exceeds the subscribed SLA availability standard, the high availability cloud architecture will route the service vial alternate data center resources functioning properly.

Reduce Manual Efforts

Modern IT infrastructure systems are inherently complex. Adding multiple layers of security and networking to connect geographically dispersed IT resources makes the architecture more complex. Relying on specialized skills and workforce may be a limitation for small and midsize businesses pursuing accelerated growth but lacking these resources to tackle the risk of unplanned downtime due to natural disasters. To address this challenge, a degree of automation should be available to implement resilience operations and failover plans. Based on a pre-planned disaster recovery strategy, the applications should be configured to resume operations from alternate nodes and access copies of business-critical data assets stored in alternate storage resources. Relying on intelligent technologies such as machine learning based IT operations and disaster recovery solutions can help organizations proactively mitigate the risk of disasters. These technologies continuously monitor for patterns of application and infrastructure performance that highlight possible disaster and trigger corrective measures accordingly. While most natural disaster situations are abrupt and may cause sudden power outage, intelligent automation systems will ensure that the corrective measures are adopted without wasting time on manually assessing the situation and responding only after the disaster has occurred.

Test for Real-Life Scenarios

The functionality and validity of disaster recovery and risk mitigation strategies should be considered on an ongoing basis. It is very much possible that a thorough strategic plan for today's risk situations may not deliver under real-life disaster situations that occur unexpectedly in the future. The disaster recovery plan should be designed to preserve business continuity under such unforeseen circumstances and the effectiveness of the plan can only be determined under testing for real-life scenarios. The basic elements of a disaster recovery testing strategy include scheduling, documentation and the feedback. Regular testing procedure help gauge the effectiveness of the disaster recovery plan under situations that tend to change rapidly. Documentation ensures that the learning from every test program are noted for future use cases. The feedback loop connecting back to the disaster recovery planning phase ensure that the risk mitigation strategy improves on a continuous basis. These testing programs should be designed to carefully improve the disaster recovery and risk management capabilities from a technology perspective. From a people's perspective however, it's likely that the workforce may not follow the playbook with equal consistency under stress during a real-world disaster situation. This gap should also be accounted for during the disaster recovery planning phase where additional measures can be applied to manage risk during the actual disaster.

Perhaps most importantly, organizations must understand the reality of the risks associated with natural disasters facing their business and their ability to respond. If this understanding is not developed accurately, a disaster situation may lead to an unpleasant surprise for the business. Failure to respond may accordingly lead to tangible loss to the business.