Refreshing the public sector disaster recovery plan

Every state government has some sort of disaster recovery (DR) plan. Unfortunately, disasters come in many forms. Some disasters are natural and others are man-made. Man-made disasters include more recent threats such as ransomware attacks. IT resources and the associated data and applications can be rendered inaccessible for a variety of reasons in a disaster.

As the potential threats mount, it is an optimal time to refresh DR plans and the thinking on which they are built.

Challenge: Maintain public services and data access in a crisis

The need for DR plans is not new. Hurricanes and other disasters wreak havoc on people and economies. IT resources can aid in the overall recovery, but only if those resources are up and running in a timely fashion.

The threat landscape evolves along with available technologies and approaches that can drive the DR plan. Are there gaps in the plan based on new developments? For instance, there could be a lack of automation, driving the need for human intervention that could delay recovery. New technologies and service models could help simplify and streamline recovery options.

Are there costs that could be mitigated with new approaches that were not available when the DR plan was first created? For instance, state governments understandably want to maintain their data within the state borders. This introduces certain contingencies worth considering and planning around. Is it cost effective to maintain complete data centers in two different regions just for the purposes of DR?

> New technologies and service models could help simplify and streamline recovery options.

Complete data centers involve capital costs and the needs to manage systems and software as well as keep those technologies up to date. If DR is the reason for doubling those costs and concerns, it is worth thinking about other ways to get the same peace of mind without the cost.

Isn't it possible that a state-wide event could occur affecting all regions simultaneously? An unprecedented storm can knock out power in many localities all at once. Likewise, dual data centers that are copies of each other could make the backup facility equally vulnerable to the same cyberattack such as a ransomware incident.

In refreshing a DR plan, it can be useful to brainstorm plausible situations where a backup data center is no safer than the main facility.

Solution: Edge compute creates new strategies for modernizing DR plans

Edge computing might not have been available when a DR plan was first created. However, Lumen's extensive network of over 40 edge compute facilities across the country creates new strategies for resiliency in an evolving threat landscape for the public sector. DR can be shifted into a Lumen facility in your state or nearby.

With Lumen® Edge Computing, DR backup can be shifted to an operating expense, alleviating capital costs. This also frees up management mindshare and the need to maintain upgrade plans under the relenting pace of technology advancement.

Results: Lower capital costs and new DR resiliency

State IT managers maintain complete control over resources and raise their ability to stay resilient in an unpredictable world. Benefits include:

- IT managers stay focused on citizens and innovating services, not maintaining DR backups
- Reduce capital costs by shifting DR to an operating expense

Edge-based computing is a key addition to DR planning and the continued modernization of state government IT.

Visit lumen.com/edgecomputing for more information.

LUMEN®
TECHNOLOGIES