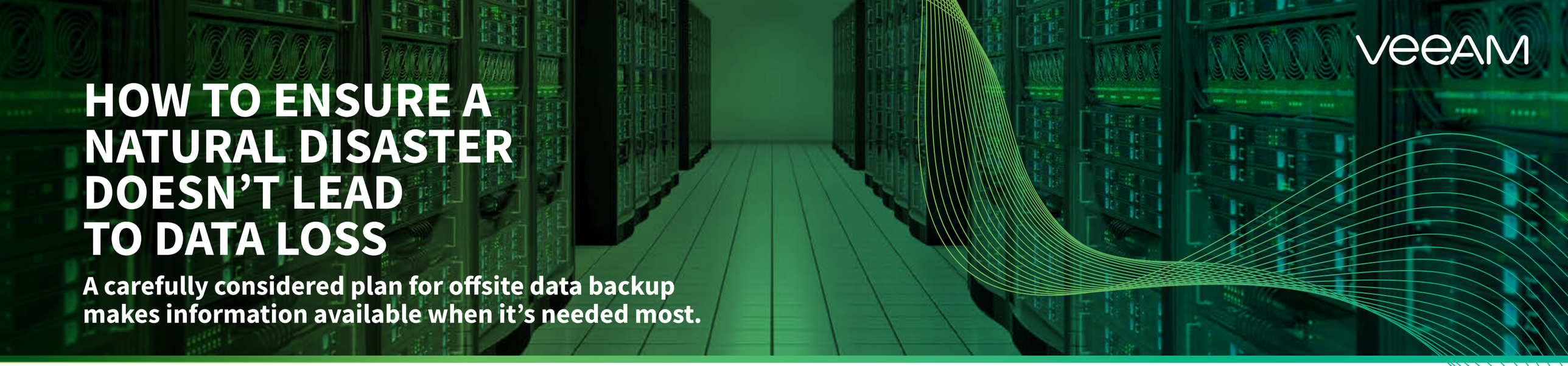

HOW TO ENSURE A NATURAL DISASTER DOESN'T LEAD TO DATA LOSS

A carefully considered plan for offsite data backup makes information available when it's needed most.

Access to data is one of the first things a government needs following a natural disaster. Data in many forms is essential to bring back government operations, deliver emergency services and help the community rebuild.

Many governments follow solid practices for creating data backups but may not have an easy or secure way to store them offsite. In other cases, a government may have offsite storage in a nearby data center or service provider's colocation facility. However, that backup is vulnerable to the same tornado, hurricane, earthquake or other widespread and destructive incident as the primary storage.

In addition, traditional tools and processes for data backup and recovery are often manual — making them slow, cumbersome and vulnerable to human error. This challenge expands as governments store data across multiple, diverse applications and storage systems, both on premises and in the cloud.

A carefully considered choice for offsite backup, a documented data recovery plan, and the right management tools and processes can help ensure vital informaton is available after a disaster. Yet many governments have found developing these resources daunting given the large scope of data and applications.

THE NEED FOR OFFSITE STORAGE

To safeguard data in the event of a natural disaster, government agencies need to ensure they have strong offsite data backup, replication and recovery services. The offsite location should be far enough away to ensure it's not susceptible to the same natural disaster as the original location. For example, when Hurricane Dorian struck in September 2019, it caused widespread damage in the Bahamas, along the U.S. eastern seaboard and into Canada. Storing data in a neighboring city or county, therefore, may not always be enough.

Other offsite storage considerations:

- Weigh the use of other locations within the organization versus colocation, a managed cloud provider versus a public cloud provider, or possibly a combination of multiple providers. Other locations or colocation typically provide the utmost flexibility for disaster recovery options.
- Copy all backups offsite. A good offsite backup is automatic, consistent and reliable. Agencies should check their offsite files regularly to make sure backups are completed consistently and perform regular disaster recovery drills to ensure all data is accessible, usable and up to date.
- Use runbooks and orchestration when available. Orchestration ensures that critical servers, applications and their dependencies come online without incident. It's important to understand how a vendor plans to failover your applications, and then failback, and how much customization and control you have in the orchestration process. Some disaster recovery providers offer runbooks that describe the order in which your systems should recover. Runbooks can help enhance IT operations efficiency measures, reduce mean time to repair, increase mean time between failures and automate the provisioning of IT resources.
- A cloud-based offsite storage solution, when and where appropriate, can provide economical offsite data backups and a comprehensive recovery service for all data files, applications and servers. This can enable advantages such as backup redundancy and multiple recovery points for reliable restoration of critical data needed to continue operations, automation to assure fast and timely backups and restores, and improved visibility and management control for protecting data from all sources (including user endpoints and software-as-a-service [Saas] applications).

TIPS FOR CREATING STRONGER DATA PROTECTION

Consider the following three tips to implement strong data protection measures.

First, look for vendor software tools that help create a detailed disaster recovery plan and automation runbook. Make sure these resources are specific to the agency's applications and data, and schedule regular reviews to keep them up to date. The plan and runbook should specify the following:

- **What is covered by the backup.** Identify backup coverage for virtual and physical servers, data storage systems, desktops and laptops, cloud applications and infrastructure, and SaaS workloads. Current business and operational data may need a more stringent plan than archived data. In addition, consider the data recovery requirements of key departments and functions such as emergency management, police and fire, and public works.
- **Replication.** For each defined workload, determine whether server replication is needed to obtain an extra measure of protection and assure timely recovery through instant failover.
- **Compliance.** Evaluate how the backup solution and processes meet regulatory requirements. Factors such as restore time objectives (RTO) and restore point objectives (RPO) for specific systems and databases may be important compliance mandates.
- **Management.** Identify the capabilities needed for data protection monitoring, reporting and capacity planning. These capabilities are essential to balance data protection, backup and recovery performance, and costs.

Second, automate backup and restore processes. Automated processes improve the timeliness and consistency of backups and reduce the potential for human error that can impair full and accurate data restoration.

Finally, automate testing of all items in the data backup, replication and recovery plan, using multiple scenarios to verify complete backups and restores. These scenarios should include all anticipated natural disasters and running automated and manual data restores. Additional items to test include:

- Operation of needed systems, applications and network connections
- Documented policies and procedures
- Team, vendor and employee roles
- Achievement of the defined RTO and RPO metrics

DATA WHEN IT'S NEEDED MOST

Today's resources for offsite backups offer powerful tools to protect government data and applications used in both every day and emergency operations. With reliable availability of information, agencies can better maintain services, protect public safety and help citizens in times of need.

HOW YAKIMA COUNTY PROTECTS PUBLIC SAFETY DATA

Emergency personnel need immediate access to essential data to protect their community during and following a natural disaster. To solve this challenge, Yakima County, Wash., implemented a cloud solution for dependable and high-speed backup, replication and recovery of 50 TB of data. The new cloud solution eliminated the frustration of failed backups that occurred with the county's previous solution. It also eliminated the time the county's server administrator spent troubleshooting those problems each week.

Another benefit: A replication design under the previous solution wasn't feasible because it required a high capital investment. Using cloud, Yakima County can economically replicate critical data for quick failover and data access in an emergency.