4 BEST PRACTICES FOR STATE AND LOCAL GOVERNMENT DISASTER RECOVERY PLANNING

A robust disaster recovery plan can help agencies protect data from ransomware and other threats.

In 2016, a ransomware virus took control of the desktop computer of a city of Sarasota, Fla., employee. The virus encrypted three servers and 160,000 files, rendering them inaccessible, as cyber criminals demanded up to $33 million in Bitcoin as ransom.

Unfortunately, Sarasota's experience isn't unique. The U.S. Department of Justice estimates more than 4,000 ransomware attacks have occurred every day since the beginning of 2016, and government is a prime target.[1] According to a recent Bitsight report, government agencies had the second-highest rate of ransomware and the second-lowest security rating among six industries examined.[2] Given such risks, a robust disaster recovery and data protection plan is critical for any state or local government organization.

Disaster recovery and data protection are especially important as agencies push more services online. Today's employees and citizens expect always-on availability and access to online services.[3] In fact, 73 percent of citizens say they expect the same or higher quality from government digital services as they do from the private sector. Agencies are responding to the demand, but that convenience can be costly if data isn't protected.

Regulatory compliance and e-discovery requirements are another reason state and local government agencies need to take data protection and disaster recovery seriously. As agencies continue to move critical applications like email to the cloud, they need to maintain control, visibility and access to data.

This brief explores four best practices for data backup and recovery.

1. IMPLEMENT AN AUTOMATED BACKUP SOLUTION

When Smoky Lake County, a municipal district in Alberta, Canada, began providing almost all services to residents on virtualized Microsoft Hyper-V systems, its data backups slowed, and county officials found it difficult to ensure those backups were successful and ready to implement if needed.

"I had no confidence in my ability to recover from a backup," says Brian Niziol, IT technician for Smoky Lake County. "We're required by law to keep all email correspondence, and I worried about being able to recover emails from our Microsoft Exchange backups."

Manually monitoring a backup system leaves room for human error. To address this issue, Smoky Lake

Government had the second-highest rate of ransomware and the second-lowest security rating out of six industries examined.

County implemented an automated backup solution with set-and-forget capabilities. Backups now occur automatically, while verification alerts let Smoky Lake County IT personnel know when backups are completed and data is saved.

2. TAKE A 3-2-1 APPROACH TO DATA STORAGE AND RECOVERY

Sarasota recovered its data without paying the ransom, but IT leaders learned a critical lesson in the process — following the 3-2-1 practice is essential to effectively recover data.

The 3-2-1 backup rule recommends organizations maintain:

- 3 copies of data
- 2 of those copies on different media, such as disk and tape
- 1 copy of data backed up off site

"Our job is to help keep city services running 24x7, particularly in the event of a crisis," says Herminio Rodriguez, Sarasota's IT director.

It's also important to keep a copy of data stored separately so if the network goes down or suffers an attack, the agency can recover its data.

3. ENSURE STRONG DATA RECOVERY CAPABILITIES ARE IN PLACE

Employees and citizens depend on government agencies to provide access to the data and services they need. But if an agency suffers an attack, their focus must move to business continuity and data recovery.

Data recovery relies on three critical capabilities:

- ✓ **Rapid recovery.** The solution deployed for data recovery should recover files within a few hours or less. Any longer is too long for any agency, and especially for any agency that oversees essential services like emergency or health services.

- ✓ **Verified recoverability.** Guaranteed recovery of every file, application or virtual server provides confidence that the entire system can be brought back online quickly.

Recovery verification can also simplify demonstration of data compliance during annual audits.

- ✓ **Office 365 mailbox data restoration.** An agency should ensure its recovery solution allows it to maintain control of email data and that data can be recovered at any time. Office 365 backup enables backup of email data in the same format Microsoft Exchange uses natively to make it easier to access email. It also ensures an agency can remain in compliance with e-discovery requirements should it encounter a cyber-attack or hard drive failure.

4. CONFIRM COMPLETE DATA VISIBILITY

Providing citizens and employees always-on availability means having complete visibility of infrastructure and data, as well as the right backup and recovery processes. An effective monitoring tool should:

- ✓ **Collect the right data.** A monitoring tool can provide the performance data agency leaders need to make decisions on how to best allocate resources.
- ✓ **Monitor multiple environments.** The ability to manage backup functionality for virtual, physical and cloud-based workloads from a single console makes it easier to manage data protection processes.
- ✓ **Provide real-time issue discovery.** A monitoring solution should include alert tools to ensure instant notification.

HOW TO STAY AHEAD OF DISASTER

Sarasota avoided paying millions to cyber criminals because it employed effective disaster recovery practices. By following the 3-2-1 rule for data storage, Sarasota ensured backups were consistent and successful and was prepared with a rapid data recovery solution. Its plan provided end-to-end visibility to monitor and effectively respond quickly to a crisis.

"If we hadn't been able to recover our files, we would have had massive data loss affecting all facets of the city and ultimately, it would have impacted our citizens," says Rodriguez.

TEST, TEST AND TEST AGAIN

Trusting a data management solution to function as promised is not enough. Running standardized, well-documented tests that consistently achieve accurate and comparable results gives agency leaders confidence they can maintain non-stop business continuity in a crisis.

In addition to monthly or quarterly tests of backup and recovery processes, agencies should consider testing in the following situations:

INFRASTRUCTURE CHANGES.

Planned or unplanned changes to the IT infrastructure can impact backup and recovery systems. Therefore, it's important to test after any infrastructure change to ensure everything is operating correctly.

UNEXPECTED OR UNUSUAL EVENTS.

Whether it's preparing for a natural disaster, a new type of cyber-attack or a hardware failure, it's a good idea to simulate various scenarios and test under those conditions.

ATYPICAL BACKUPS.

Test for instances where backup and restore processes are required to be completed differently than they typically would. For example, test with a manual backup restore as well as an automated restore.

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Veeam.

Endnotes

1. "New Research Shows Ransomware Is Not Just In Healthcare: Education and Government Sectors Experience Highest Rates of Attack," Bitsight, September 21, 2016, https://www.bitsighttech.com/press-releases/new-research-shows-ransomware-is-not-just-in-healthcare.
2. Ibid.
3. "Digital Government: Your Digital Citizens are Ready, Willing…and Waiting," Accenture, 2016, https://www.accenture.com/t20160309T122224__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_7/Accenture-Digital-Government-Your-Digital-Citizens-Ready-Willing-Waiting.pdf.

PRODUCED BY: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government is a national research and advisory institute focused on technology policy and best practices in state and local government. The Center provides public- and private-sector leaders with decision support and actionable insight to help drive 21st-century government. The Center is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.
www.centerdigitalgov.com

SPONSORED BY: VEEAM

Veeam recognizes the challenges governments face in enabling the Always-On Enterprise™; business that must operate 24.7.365. Veeam has pioneered a market of Availability for the Always-On Enterprise™ by meeting recovery time and point objectives (RTPO™) of less than 15 minutes.
www.veeam.com