Increasing government resilience with cloud-based disaster recovery

As state and local governments increasingly rely on cloud services, they have a responsibility to protect their data and ensure their systems are secure. This starts by understanding current practices and solutions are not always secure by default and developing best practices to mitigating new risks that may emerge in the future.

While many state and local governments are making progress to strengthen enterprise security, their efforts must focus not only on prevention, but also robust disaster recovery. By moving disaster recovery to the cloud, state and local governments can reduce time and lower cost to recovery while ensuring mission-critical applications and services are available when constituents need them most.

Last fall, ransomware on a web hosting provider forced the company to take its servers offline, causing several state and local government websites across the country to be inaccessible. The pandemic has also increased the threat landscape. Sixty-one percent of local governments have reported an increase in cyber threats since the beginning of the pandemic, according to recent research from the Center for Digital Government (CDG) and Amazon Web Services (AWS).

State and local government organizations can improve IT resilience with cloud-based disaster recovery while strengthening their overall security posture to combat ransomware threats.

Disaster recovery challenges in government

State and local governments face several challenges when it comes to disaster recovery. Alex Berkov, manager of solutions architecture for CloudEndure Disaster Recovery, offered by AWS, a leading cloud-based disaster recovery and business continuity solution, says there’s often confusion about what disaster recovery actually encompasses.
“There is a lot of misconception around the difference between backup and disaster recovery. Often what customers call disaster recovery is actually backup,” he says. “State and local governments need to ensure security controls are also in place for backups as these backups can be impacted by ransomware.”

Many organizations also cannot adequately test their environment, Berkov adds. They may not do frequent testing from their backups or they may rely on traditional disaster recovery solutions that require them to spend weekends in a physical data center to run tests. State and local agencies also might rely on a magnetic tape backup solution where they dump data out, back it up, and then save it on a physical tape.

All these processes are so labor- and time-intensive that organizations might only do them on an annual or infrequent basis, which leads to inadvertent security gaps. These security gaps are costly for government agencies and can lead them to pay ransom to help achieve business continuity for critical constituent services. In 2019, governments reported 163 ransomware events, with more than $1.8 million dollars in ransoms paid. In 2020, these figures only increased, as outside parties demanded an average payment of just over $570,000, with requested ransoms ranging from $2,500 to $5 million.

Garrett Pollard, a senior enterprise sales specialist for CloudEndure Disaster Recovery at AWS, says it’s critical for governments to have a comprehensive continuity strategy given IT’s increasing value to the business.

“It supports so many different revenue streams that any downtime may pose a significant loss,” Pollard says.

It’s clear the traditional approach to disaster recovery doesn’t give state and local governments the agility they need to quickly and effectively respond when security issues occur.

**Optimizing operations with the cloud**

Moving disaster recovery to the cloud offers cost and operational benefits to state and local governments that can improve their resiliency.
the solution can do all the replication, management, and orchestration of their resources,” Berkov says.

Some organizations are already seeing improved operational impact from cloud-based disaster recovery. One state agency, for example, experienced a ransomware event that affected its entire on-premises infrastructure, including a database that contained all its employees’ password information. Backups for the agency’s business-critical applications were also compromised during the event, leaving it without any backups from which to recover.

Rather than undergo a lengthy hardware procurement process and entirely rebuild its data center, the agency decided to shift its entire IT operation to the cloud. It was able to restore all of its mission-critical applications in a cloud environment in less than two weeks. The agency also has realized significant cost savings — it is now running its IT operation at 40 percent of what it would cost to run it on premises.

Best practices for moving disaster recovery to the cloud
Disaster recovery in the cloud addresses several key challenges for state and local agencies by providing a flexible, scalable solution that can reduce time and lower cost to recovery while helping to address budget constraints and minimize unintended security risks. State and local agencies should consider the following as they transition to cloud-based disaster recovery and compare solutions.

Establish recovery time objectives
Before a state or local agency enlists the services of a cloud provider, they should clearly map out and understand their disaster recovery needs, Pollard says.

“The cloud really does, from a scalability perspective, give organizations the option to right-size their disaster recovery environment.”

Alex Berkov, Manager of Solutions Architecture for CloudEndure Disaster Recovery

“Sit down and take a hard look at your business and establish what your recovery time objectives are for each application. It’s a very common exercise where you take a step back, analyze the data, and see what the recovery times are so you can figure out which solution is the best fit,” he says.

Plan for flexibility and scalability
“You need to make sure the solution is effective not just for today, but can handle any future growth,” Berkov says. “The other thing you need to consider, particularly when it comes to ransomware, is the flexibility and insurance of having different recovery forms. That way, if you are hit by ransomware, your organization can go back to a previous point in time just as quickly as you can fail over.”

He adds: “The cloud really does, from a scalability perspective, give organizations the option to right-size their disaster recovery environment. You don’t need to over-provision anything — it’s scalable and it’s elastic — you only use what you need.”

Ensure data governance and compliance
Whether an organization operates on premises or in the cloud, good data governance is critical to effective disaster recovery.
It’s important for government organizations to have compliance across all of their workloads, which is why they should work with a cloud provider who has public sector expertise and a solid track record of managing these types of workloads.

Perry says some of the questions organizations should ask potential cloud providers include: “How do you encrypt the data in transit? How do you encrypt it at rest? How can we make sure that only the right people have access to the data? They’re [government agencies] often learning about how the cloud operates and all of the compliance benefits it provides. So, there’s a learning process, and how to extend their governance processes, auditing, and monitoring [activities] to the cloud is part of that.”

**Test, test, test**

Testing is critical when it comes to disaster recovery.

“You don’t want to wait until an event happens before you test,” Berkov says. “The cloud opens up the ability for you to test on your own schedule at any time with really no impact. It also allows you to increase the frequency of those tests, so you can make sure that, as your environment changes, you can validate it and verify everything is running properly.”

**Conclusion**

From ransomware and malware to email phishing schemes and denial-of-service issues, security threats continue to impact state and local governments.

As these organizations try to build a more robust cybersecurity program, effective disaster recovery should be an integral component of their holistic cybersecurity strategy. The traditional approach to disaster recovery — with backups from magnetic tape and a reliance on on-premises data centers — can be costly and time consuming for state and local governments facing budget cuts and limited IT resources. Government organizations can leverage the cloud to modernize their disaster recovery program and make their IT operations more cost efficient. By doing so, they can improve business continuity and build their resilience.

“The challenge state and local governments face is they often don’t have IT staff or security experts to build disaster recovery processes internally and execute them in a consistent way on premises,” Perry says. “One of the greatest benefits of the cloud is that the services you need to combat ransomware — whether it’s patch management, encryption, firewalls, or intrusion detection — are provided as managed services in the cloud. They’re integrated so you have a toolbox that’s been built to work together to greatly simplify the IT complexities and challenges your organization faces.”

For more information about AWS, please contact us.

This piece was developed and written by the Government Technology Content Studio, with information and input from AWS.

---

You don’t want to wait until an event happens before you test. The cloud opens up the ability for you to test on your own schedule at any time with really no impact.

Alex Berkov, Manager of Solutions Architecture for CloudEndure Disaster Recovery

---

Footnotes