Disaster Recovery in State and Local Governments
Disaster by the Numbers

- Over 70% of agencies had some sort of data loss incident in 2012
- Under 5% report that they were able to recover from their incident in under an hour
- A 2015 Carnegie Mellon University study found 10% of flash drives spawned occasional errors while in use.
  - Study of disc drives 9 years earlier found 4% failed prematurely
- We estimate that government agencies lose over $70 million in man hours or business functionality each year due to data loss and dealing with system and data recovery
IDC: How Much do Organizations Spend on DR Strategies?

Worldwide Data Protection and Recovery Software Revenue by Region, 2016 and 2021

State/Regional and Local governments represent about 8% of this spending

Source: IDC's Worldwide Semiannual Software Tracker, May 2017
Building Disaster Recovery Into Your Digital Plans

- Be prepared - Characteristics of an effective DR plan include the following
  - Ensure full recovery of your agencies entire computing environment
  - Resume operations quickly and smoothly
  - Work to achieve continuous synchronization of data
  - Recovery Time Objective (RTO) of 15 minutes or less, and a Recovery Point Objective (RPO) of 30 seconds.
  - Recovery occurs across virtual, physical, and cloud systems
  - Ability to easily and regularly conduct test failovers for assurances
  - Goal is to assure not just disaster recovery, but business continuity.
Disaster Recovery is Challenging for State and Local Governments – For Many Reasons

- High cost for data facilities, especially acquiring facilities outside of an agency’s geography in order to address geo-redundancy
- High capital investment for (and the need to refresh) duplicative hardware, software licenses, and other computing infrastructure such as networking gear for the DR site
- SLG is starting to rely heavily on IOT and intelligence of systems/applications for daily operations - the level of data (and associated business functions) that reside on government networks is exploding
- S&L governments need disaster recovery at a size or scale that can be difficult to achieve in a self-hosted environment
- Meanwhile, agencies are increasingly dependent on accurate data for digital transformation initiatives. In turn, this has sparked investments in data protection technologies, along with a desire to reduce complexity in IT environments
- There’s pressure to set recovery time objective (RTO) targets for each system on the agency’s network
- Compliance is one of the challenges that agencies often cite when choosing to move their backup and DR activities to the cloud
Disaster Recovery in State and Local Governments

▪ Look for a service provider who understands government data needs, and how agencies license their solutions
▪ Seek minimal financial investment and zero lock-in. Many DR solution providers offer pay-as-you-go cloud-based subscriptions
▪ Work with key systems integrators to help build robust and reliable solutions
▪ What is your tolerance for failure? (Recovery times, potential data loss levels, employee hours spent, etc.) This determines cost of the solution
Recovery Example

Cloud-based Orchestration for Site Recovery

Primary Data Center

Secondary Data Center
Disaster Recovery’s Place In Maintaining Continuity of Government Functions and Services

- Data protection and recovery is one of the strongest areas for data center investment by government agencies.
- Government continue to invest in both onsite and cloud-based solutions. But cloud-based DR is the trend and logical approach.

- Backup-as alone is not a DR solution
- Full automated roll-over recovery may be appropriate for large agencies with detailed transaction-based data sets, and can still be cost effective for small and medium-sized agencies
How much does an hour of downtime cost your organization?
ROI analysis should focus on potential loss of productivity.
Partner ecosystem – can your system integrator help you tap into top-level disaster recovery?

Many government agencies work toward data protection as a service (DPaaS).
This includes the following:
• Backup as a Service (BaaS)
• Archive as a service (AaaS)
• Disaster recovery as a service (DRaaS)
Current non-Cloud strategies

- Government Agencies often buy and install their own data back-up and recovery solutions
- This means they are responsible for all upkeep, patches, monitoring, troubleshooting etc.
- They are responsible for keeping redundant geographically disburse systems

Drawbacks
- Capital investment for hardware infrastructure
- IT department has direct responsibility for business continuity
- Staff must maintain expertise in a variety of technologies that may shift over time
- Budget fluctuations can affect performance and upgrades
- Can’t take advantage of economies of scale
Government agencies are looking to implement best of breed disaster recovery solutions

Agency leaders and CFOs need to understand the importance of assessing the risks associated with downtime agency business functions, and they need to help create a plan to avoid it.

In local environments, downtime can even mean **loss of life** if SLG organization cannot respond with critical services.

No city or state government is immune to the issues associated with natural or man-made disasters. Downtime = costs and loss of functionality, which can bust an annual budget by millions of dollars.
Disaster Recovery Best Practices

- Maintain one or more copies of all mission-critical data outside of your main computing facility production region
- Test your agency’s business continuity/disaster recovery plan in a credible way to ensure it has full functionality
- Be realistic about the service level agreement you will need, and make sure it is properly supported
- Make sure your continuity plan is accessible and capable of being executed in the event of a major disaster
- Make sure multiple people trained in the steps of your continuity plan, including someone outside of your regular agency locations
- Is your DR provider also geographically redundant? It’s important that they are
Azure Government’s Role in Government Business Continuity

- Capable of unifying data management, security, and protection
- Offers a set of solutions to support continuity and compliance, with full lifecycle considerations
- Helps promote data security, and additional protection via encryption
- Offers a Hyperscale Cloud with large geo-redundant data centers whose primary business is the intelligent cloud
- Focused on a disaster recovery solution that protects and natively supports the widest range of enterprise applications of any cloud disaster recovery provider.
Azure Government’s Approach to State & Local Disaster Recovery

- Allows even the smallest local governments to obtain high-end security, protection, and compliance
- Provides an opportunity to modernize hardware infrastructure that may be reaching end-of-life
- Supports hyperscale
  - Seamlessly provisioning systems, and add compute power, memory, networking, and storage resources as needed
- Offers system redundancy at a level that meets most U.S. common federal, state and local requirements for disaster recover and data safety
Next Steps Toward Disaster Recover

- Inventory of current systems that need disaster recovery solutions
- What do your current solutions cost? What is the expected life cycle
- Conduct an ROI analysis – current solution vs. migrating to Azure
- You likely have a Microsoft Account Team – this team can conduct a DR proof of concept using Microsoft Azure
Advice to State and Local Government Agencies

- Disasters are “local” by their very nature.
- Have a disaster recover plan in place well before the disaster happens.
- Disasters come in many flavors (hurricanes, water damage, fires, loss of network connectivity, insider threat and more) have a disaster recovery plan that addresses all of these.
- Situational dashboards and real-time reports can help managers make informed recovery decisions.
- Redundant network connectivity is as important as other system redundancies.
Azure Site Recovery (ASR)
Overview of solution architecture, concepts, and scenarios
Introduction

- ASR is a Disaster-as-a-Service (DRaaS) solution, formerly InMage.

- It can be used for DR and/or migration to Azure.

- ASR should be used in conjunction with a backup solution (e.g. Azure Backup) to meet the technical needs of a comprehensive Business Continuity and Disaster Recovery (BCDR) plan.

- ASR is not dependent on a dedicated connection such as ExpressRoute.
Recovery Time Objective (RTO)

• How quickly is IT expected to bring up systems affected by an incident?

Recovery Point Objective (RPO)

• In the event of an unexpected incident, what is IT’s SLA on how much data is at risk of being lost?
• ASR provides two configuration options:
  ➢ 30 seconds
  ➢ 5 minutes
  ➢ 15 minutes
Protected Instances

- The server(s)/VMs that are protected via ASR

A remote DR site “close by” usually does not meet industry standards:
- Microsoft has adopted the 500 miles or more approach.
- Need to be a completely separate facility from primary facility.
- Cannot share same public/telco utility infrastructure.
- Must be geographically diverse and not share same risks (e.g. on the same fault line).
- DR Site must have true 24x7x365 operational standard.
- Redundant personnel that will not all be affected by an incident.
- Must also meet Federal, State, and Local government regulatory compliance standards.
ASR and Backup are not mutually exclusive and should be used together as part of a comprehensive BCDR plan.

### ASR vs Backup use case scenarios

<table>
<thead>
<tr>
<th>Feature</th>
<th>ASR</th>
<th>Any backup solution (e.g. Azure Backup)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTO = 0 to minimum</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>RPO = Within seconds or minutes</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Archiving (long term)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Retention (short to medium term)</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

---

*ASR and Backup are not mutually exclusive and should be used together as part of a comprehensive BCDR plan.*
ASR Replication Process

Phase 1 – Initial Replication (IR)
Phase 2 – Post Replication
Phase 3 – Delta Replication
Phase 4 – Resynchronization\(^1\)

\(^1\)Only as needed
ASR Scenarios

Physical

Primary site (on-premises)

vSphere
Microsoft Hyper-V

Secondary site (on-premises)

Microsoft Azure

Recovery Services Vault

VMs (Protected instances) - OFF

Azure Site Recovery

Or
ExpressRoute

Internet
Demos
Thank you for joining us.