Weathering the Storm:
How Your Non-Profit Can Build a Viable Disaster Recovery Plan Using the Cloud

December 6, 2018
Housekeeping

Close any programs that are running on your computer (other than GoToWebinar)

Use one monitor for the webinar

If you experience visual or audio issues, please contact GoTo at https://support.logmeininc.com/gotowebinar/contactus

If you have any issues, don’t worry! We will send you the recording after the webinar.
Ask Questions!

- To ask our presenter questions, please use the GoToWebinar panel on your screen.
- Please enter your question here and click SEND.
- We will answer as many questions as time permits or follow up after the webinar.
About the Presenter

Greg Inks, Cloud Practice Lead
AKA Enterprise Solutions

With two decades specializing in Microsoft and Azure platforms, Greg is a Cloud evangelist, with deep expertise in Cloud architectures and adoption strategy. He has developed subject-matter expertise and wide-ranging business acumen by working with some of the largest, most successful technology providers and client companies on the planet.
Introduction

Key Questions & Considerations
1. Why a Disaster Recovery Plan is essential for the survival of your non-profit

2. Considerations for determining a Disaster Recovery Plan

3. How affordable a Disaster Recovery Plan in the Cloud is

4. Best practices when evaluating Disaster Recovery options
## Disasters Are Easy to Avoid, Right?

<table>
<thead>
<tr>
<th>Individuals</th>
<th>Organizations</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Equipment Theft / Loss</td>
<td>- Same as Individuals, plus...</td>
<td>- Same as Organizations, plus...</td>
</tr>
<tr>
<td>- Results of Compromised Passwords / Security</td>
<td>- Local Natural Disasters, i.e.</td>
<td>- Major Natural Disasters, i.e.</td>
</tr>
<tr>
<td>- Physical Accidents / Hardware Failures</td>
<td>- Wildfires</td>
<td>- Hurricanes / Flooding</td>
</tr>
<tr>
<td>- Targeted Malware / Hack / Spam / Bad Websites</td>
<td>- Hurricanes / Flooding</td>
<td>- Earthquakes</td>
</tr>
<tr>
<td>- Inability to reach central office / Organization</td>
<td>- Extreme Heat / Cold</td>
<td>- Evacuation / Relocation</td>
</tr>
<tr>
<td>- Unintended Mistakes / Fat Finger Accidents!</td>
<td>- Power Outage</td>
<td>- Geo-political Unrest</td>
</tr>
<tr>
<td>- Dogs and Kids!</td>
<td>- Local Political Unrest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Brand Targeting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Terrorism / Bad Actors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Employees (malicious or accidental)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Internet ISVs</td>
<td></td>
</tr>
</tbody>
</table>

And the list goes on...
Ask Yourself If...

- My non-profit systems were not available to employees for 30 minutes, what is the impact?
- My employees' laptop were lost, what is my non-profit’s risk exposure? What about productivity of the employee?
- The power goes out to my data center, do I have a fall back? What about if the power goes out for the eastern half of the US?
- We are targeted by a protest, and they crash our website, how does the world reach us? How long can we stay off the web and still be effective?
- The database is corrupted by a bad actor, and I have to take it offline, what are by business continuity plans?
- The hurricane really does hit, and our building is destroyed, what happens to the people who depend on us? What about our employees?
Consider Your Initial Plan

- **Pre-plan: The best defense is preparedness!**
  - Work with your CISO (Chief Information Security Officer, or counterpart) to review your security posture
  - Consider Individual Security first... two-factor authentication, virus protection, firewall, etc.
  - Conduct security and safety preparedness training for all your employees
  - Potentially conduct white-hat testing of your systems
  - Eliminate single points of failure in all critical systems!

- **Evaluate: Unemotionally and realistically evaluate your exposure**
  - “My website is critical... it must be up 99.9% of the time” = ~9 hours of “blackout” per year
  - How much do you spend to prohibit 9 hours of “blackout” – or do you at all?
  - “If I drop my laptop, how much will it cost for a data forensics specialist to recover my data?”
  - Or worse... “if my data gets into someone else’s hands, what kind of trouble is my non-profit in?”

Assuming you have done some protection, what do you do when disaster strikes?
Disaster Recovery Options

For Individuals
Options for Individuals

- **Protect Assets**
  - Implement a container service for end-point devices like Microsoft Intune and EMS
  - Leverage individual backup solutions to prevent data loss such as Microsoft OneDrive
  - Save all organizational data to a secure file store with Microsoft SharePoint or Microsoft Teams

- **Protect People**
  - Use a multi-factor authentication solution to create much stronger security solutions than passwords
  - Use Office 365 Exchange Online for AI and Business Controlled Email / Spam protection, as well as embedded link and URL protection (Click-Bait)
Options for Individuals (cont.)

- Plans are priced per Individual and per service: use only what you need for only those that need it
- Licensing becomes subscription, so grow up and down without managing licensing keys

Example (simplified):
- Non-Profit – 100 employees
- Office 365 (Outlook, OneDrive, SharePoint) $3 to $4 / person / month (including software downloads) on 5 devices (phones, tables, laptops, Mac’s)
- Advanced Threat Protection / Intune $0.60 / person / month
- Everything is DR backed up, users are protected, email is secured for ~$300 to $400 per month
Disaster Recovery Options
For Organizations
The single largest driver of cost for DR solutions for non-profit organizations is RTO and RPO

- RTO is the calculated time you have and how quickly you need to recover
  - This drives the type of solution you will need to build, and the overall budget you should assign to business continuity
  - RPO is determined by looking at the time between data backups and the amount of data that could be lost in between backups

- These two factors weigh in heavily on how DR is built for you

- The smaller the RTO, the more of a High Availability (or multi-site, multi-server) solution you will need, as well as traditionally proportionally more expensive!

- The smaller the RPO, the more aggressive data backup solution you need in place to prevent loss, and also traditionally proportionally more expensive!
How Your Non-Profit Can Build a Viable Disaster Recovery Plan Using the Cloud
Scenario: On Premise Data Center, RTO 60 minutes, RPO 20 minutes

- Single data center, on premise or managed by a single hosting MSP
- Concerns about power failure or loss of internet at MSP – can handle an outage, but not for more than 60 minutes
- Lost power for 2 days last year during the hurricanes
- Some data loss is acceptable, but ideally minimized
- Cannot afford a duplicate MSP (not an option)
- 10 servers, approximately 10 TB of data

Potential Solution:

- Secondary DR site in Azure, as virtualized infrastructure
- Leverage Azure Site Recovery (ASR) to near real-time replicate the entire on-premise data center to Azure, in an “off-line” state

Setup Costs:

- One-time setup of Virtual Networking for Hybrid connectivity
- Setup of ASR on-premise and Azure
- Setup Runbooks and Monitoring
- Setup automation for “fail-over”

Monthly Run Costs (estimates and as an example):

- Management of Azure infrastructure (human)
- Azure storage of Data (monthly Azure spend) ~$400/month
- ASR costs (monthly Azure spend) ~$250/month
- VM run / compute – $0/month, its offline till you use it

Total: ~$650/month
Scenario: Highly Valuable Database, RTO N/A, RPO < 5 minutes

- Organization has a database that contains very important data that the system keeps up to date
- Concerns about loss of data and making sure that there is a backup with very low loss of data (including changes)
- The system can go down and work can continue, but a data loss would be severe
- Database size makes a duplicate on premise not a viable option (costly)
- Additionally, Organization has a file server with large amounts of historical contracts / grants / artifacts
- 20 TB of data

Potential Solution:

- Secondary DR storage site in Azure, as Platform as a Service
- Leverage Azure Storage Accounts to push up SQL data into BLOB storage
- Leverage Azure Storage Accounts to push up files into FILE storage

Setup Costs:

- One-time setup of Virtual Networking for Hybrid connectivity
- Setup of Azure Storage accounts for BLOB
- Setup of Azure Storage accounts for FILE
- Setup Runbooks and Monitoring

Monthly Run Costs (estimates and as an example):

- Management of Azure infrastructure (human)
- Azure Storage Account (20 TB) (monthly Azure spend) ~$400/month

Total: ~$400/month
Scenario: Mission-Critical Web Site, RTO < 5 minutes, RPO < 5 minutes

- Organization has a mission-critical web site for their non-profit for their target beneficiaries
- Downtime of site means potential for loss of life
- Organization hosts the web site on premise in their data center in Virginia
- Recent weather events have caused power outages, internet outages, and inability for organization members to make it into primary work location
- Looking for a solution that is geographically protected, always up with a 99.9% (ideally 99.99%) uptime, RTO < 5 minutes, and RPO < 5 minutes
- Organization cannot afford to build a second data center in another location distant enough to protect against geographic weather events
- Ideally, Organization also wants the solution to be more performant when reaching their target beneficiaries (for countries with poor internet coverage)

Potential Solution:

- Create a primary App Service (PaaS) for the web site in Azure in East US
- Create a secondary App Service (PaaS) for the web site in Azure in West US
- Setup an Azure Load Balancer that recognizes failure in East US and moves traffic to West US automatically
- Setup Azure CDN to distribute and cache the website static assets across the globe

Setup Costs:

- One-time setup of Azure App Services and Load Balancer with rules
- Setup of Azure CDN for content cache and site delivery
- Setup Runbooks and Monitoring

Monthly Run Costs (estimates and as an example):

- Management of Azure infrastructure (human)
- Azure App Services (both East and West US) ~$200/month
- Azure CDN (varies) ~$150

Total: ~$350/month
Paying for a Disaster Recovery Plan

How Affordable is DR in Azure?
How Affordable is Disaster Recovery in Azure?

- Previous examples showed the following:
  - For Individuals, cost is $3-4 per person per month (averagely) and provides you near complete DR coverage
  - For Organizations, you only pay for Storage and used Compute – if it’s not running, it’s only the cost of storage
  - Azure is a great alternative to expensive investment in hardware and data centers for DR scenarios

- Storage is relatively cheap for Disks, Files, Email
- Compute (VMs and Servers) are basically FREE if they are not in use
- Mission-Critical Systems can be architected so that you still use your hardware investment on premise, but leverage Azure as your “insurance policy”
  - Any combination of your existing hardware plus cloud hardware to give you DR coverage
  - Hybrid datacenter = Disaster Recovery Solution!
What does this offer cost?

- Required Pre-requisite: Executed Cloud Essentials OR Existing ARM Network Topography
- Priced per VM / SQL Database on a Volume Basis

<table>
<thead>
<tr>
<th>Service</th>
<th>Cost per (Non Managed Customer)*</th>
<th>Cost per (Managed Customer)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>2x 2-hour HADR Workshops</td>
<td>INCLUDED</td>
<td></td>
</tr>
<tr>
<td>DR Setup per VM</td>
<td>$1,000</td>
<td>$800</td>
</tr>
<tr>
<td>HADR Setup per VM</td>
<td>$1,200</td>
<td>$1,000</td>
</tr>
<tr>
<td>DR Setup per SQL Database</td>
<td>$300</td>
<td>$200</td>
</tr>
<tr>
<td>HADR Setup per SQL Database</td>
<td>$400</td>
<td>$300</td>
</tr>
</tbody>
</table>

* Prices shown assuming 10-15 instances setup

If, together, we can determine you will spend $1,500/month...

...Microsoft will give the partner up to $5,000 to use on AKA HA DR!
Next Steps

How Do You Get Started?
1. First: Contact AKA for a free Disaster Recovery Discovery Call
   - We will discuss with you what your concerns are – from individuals to organizations – and see if there is a logical fit for Azure
   - AKA will engage Microsoft on your behalf to determine if there is funding to help solve your DR problem – potentially offsetting your Azure costs or implementation of a DR solution
   - AKA will give you an initial plan on how to go about building this DR solution and an idea of costs

2. Then: AKA and Microsoft will help you get that Disaster Recovery solution in place
Questions & Answers