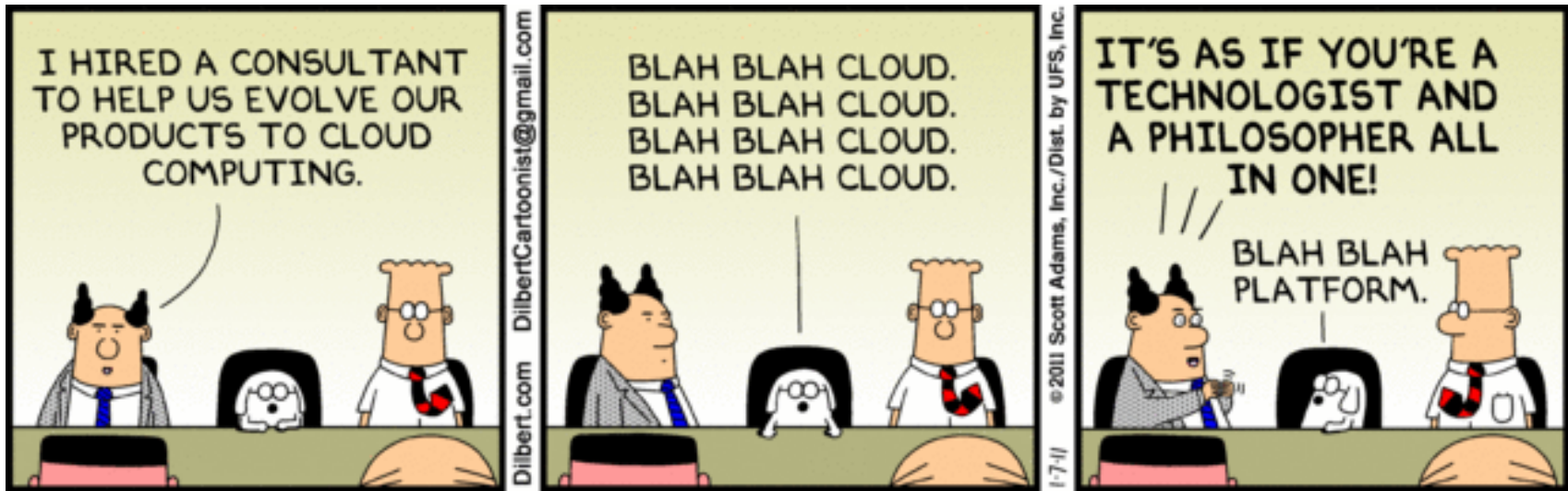


Data In The Cloud: Who Owns It, and How Do You Get it Back?

Presented by Dave Millier, Soban Bhatti, and Oleg Sotnikov

Agenda

- Reasons for Cloud Adoption
- How Did My Data Get There?
- Types of Providers, Types of Data
- Cloud Security Challenges
- Data Residency Concerns
- Quick Note on “Safe Harbor Privacy Principles”
- What Assurances Do I Have Around Data Protection?
- Who Owns my Data Anyway?
- Managing Cloud Deployments
- Research Paper: Incident Response In The Cloud
- Summary
- Questions



Reasons For Cloud Adoption

- Service Flexibility (scale IT up and down as you need it)
- Ability to rapidly turn up new systems and access storage
- Quickly deploy new services to internal and external users
- Significant Cost Reductions (on demand scaling vs pre-defined)
- No more capital expenses
- Pay as you use services, vs fixed costs for things you may never use
- Simple and effective Disaster Recovery
- Support distributed workforce (teleworkers, branch offices, etc.)



Who's Putting Our Data Out There and Why?

- Marketing
- Skunkworks Projects
- Sharing
- People working from Home
- Teams can't wait for IT to set up new Sharepoint Sites
- Free storage with a new devices (phone, tablet, PC)
- Company adopting Cloud-Based Applications
- Others?

Sample of Cloud Providers



Types of Data In The Cloud

- Email (anti-spam, archiving, business continuity)
- Documents
- Servers
- Virtual Workstations
- Projects
- Source Code
- Accounting Records
- Network Information
- Vulnerability Data
- Banking Information

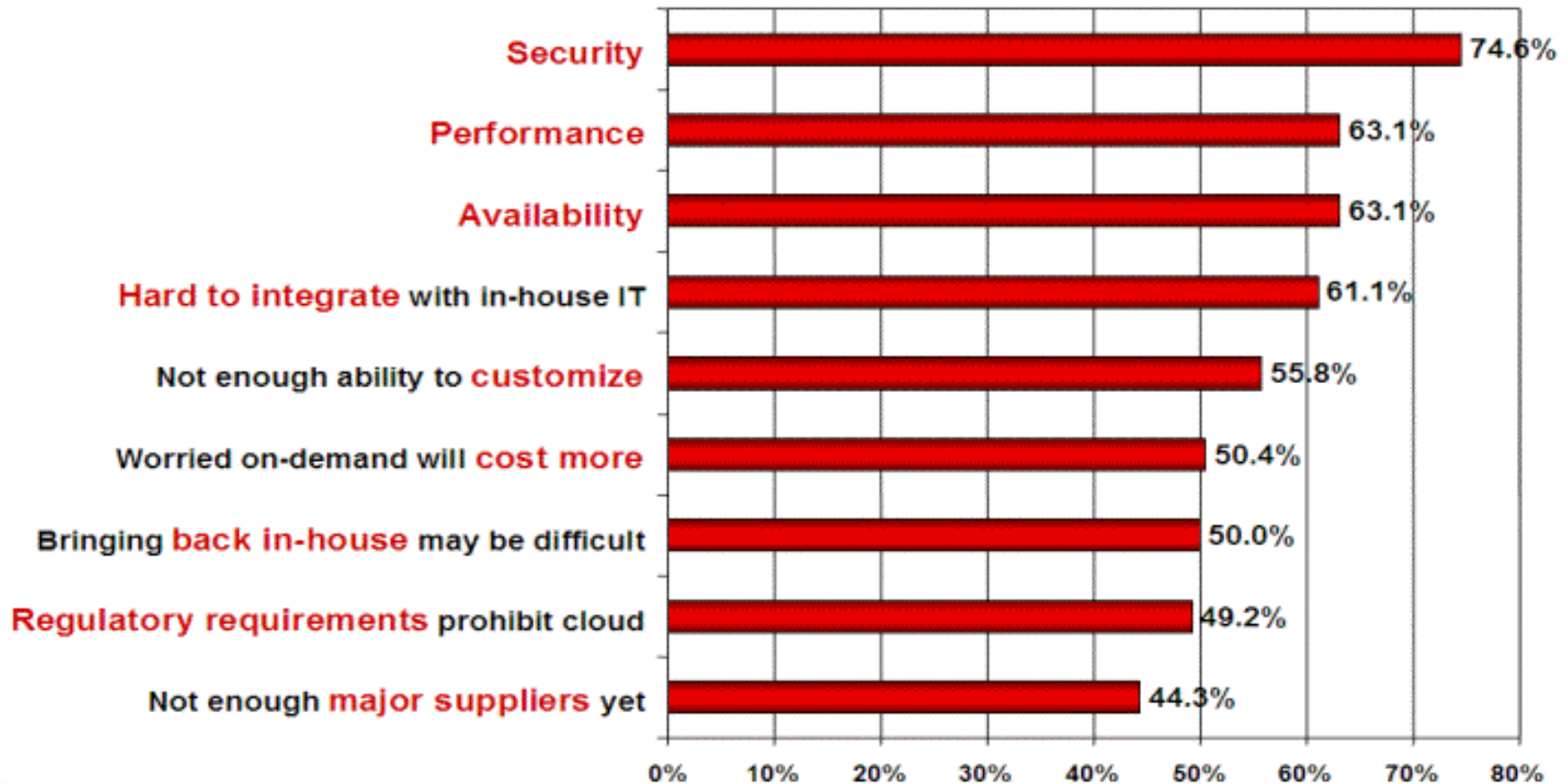
Cloud Security Challenges

- **Security of Information Stored In The Cloud**
 - Who has access to it
 - What information is stored
 - How is the information protected (from malicious users and for backup purposes)

- **Privacy Concerns**
 - Is the data stored outside of Canada (data residency concerns)

- **Visibility**
 - Is the cloud provider logging access?
 - Is the cloud provider backing up my data? If yes, where do they back it up? How many copies of my data are there out there, anyways?

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
 (1=not significant, 5=very significant)



Data Residency Concerns

- Provider is in Canada, backup takes place to another country
- Go with Canadian Service Provider, they leverage Elastic Cloud which occasionally turns up hosts in another country
- Provider assures you data will not go to the United States (Patriot Act/ PRISM concerns), but what about “their” provider?
- High Availability environments typically fall over to another geographic location, many times outside of the country to DR purposes

Security and Privacy Issues

- No client control over the things we are used to being able to manage
 - User Accounts (provider can over-ride, and has their own access outside of yours)
 - Permission on the files/folders/data in the Cloud
 - Logging of access (Providers won't give you the raw logs for real-time monitoring)
 - Visibility and Auditing
 - PCI v3 requires Service Providers to maintain the same control posture as a customer
- If we can't see who's doing what and where they're doing it from in most cases, how can we provide assurances to employees and/or customers that their privacy is protected? Just because we've moved the data to the Cloud, we haven't moved the responsibilities
- Disclosure at all times of where your data resides is required, most Providers can't/won't provide this information without a lot of digging

Safe Harbor Principles

- These principles must provide:
- **Notice** - Individuals must be informed that their data is being collected and about how it will be used.
- **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security** - Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** - Data must be relevant and reliable for the purpose it was collected for.
- **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- **Enforcement** - There must be effective means of enforcing these rules.

Whose Data is It, Anyways?

- SaaS Providers collect the data, store it, in many cases enrich the data; once they have it, and especially once it gets changed, is the data still really yours?
- Most agreements (Amazon, Google) have provisions that specifically state the provider may “use” the data to provide it to you or your end users
- From Google’s Cloud Storage Agreement:

“...to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Application and/or Customer Data for the sole purpose of enabling Google to provide, maintain, protect, and improve the Services in accordance with the Agreement.”

What Are The Providers Telling Us?

- SLAs don't provide assurance about data confidentiality, integrity, and availability (CIA)
- They aren't responsible for supporting any of your policies or your requirements (even though some regulations require it)
- It's up to you to keep your data backed up
- The Providers can't/won't access your data (but all agreements have exceptions to this!)
- They aren't obligated to protect your data in their environment
- Providers will turn data over to law enforcement upon request

Food for Thought, Managing Cloud Deployments

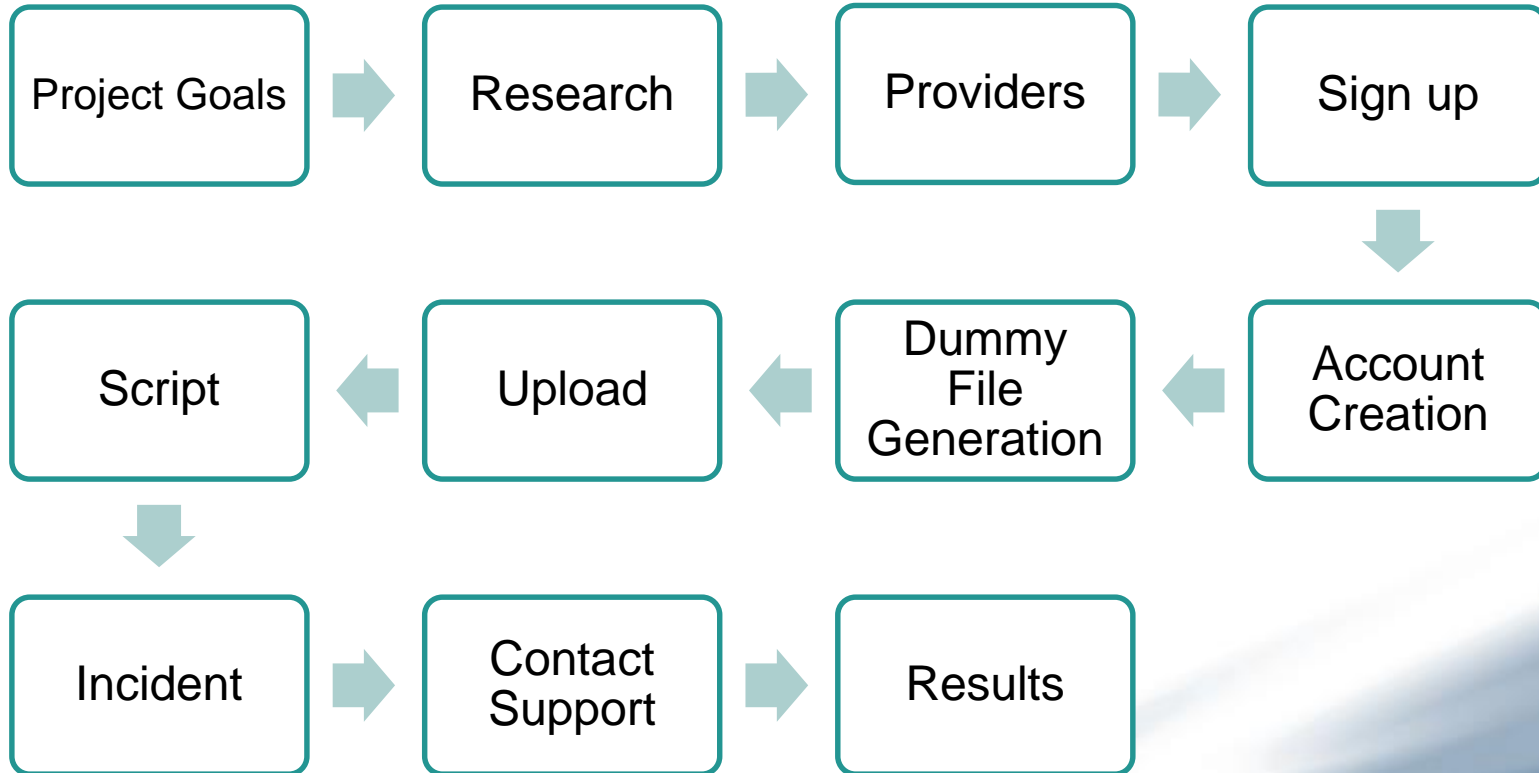
- Create an AUP (Acceptable Use Policy) and get all users to sign it prior to putting data in the cloud or using any Cloud service
- Make sure your users have to get written approval from someone knowledgeable around Cloud Services prior to signing up for a corporate account
- Ensure users know that they can't use their personal Cloud accounts to store or work with any corporate data
- Create a central repository of all Cloud services; ensure you have master login details, and maintain and update a list of any corporate data stored there
- Ensure your policy has a data destruction section, outlining when and how to remove data from the Cloud service once it's no longer required
- Use encryption wherever possible, both when communicating with the Cloud provider and if it's available on any stored data

Incident Response In The Cloud

Soban Bhatti

Oleg Sotnikov

Timeline



Providers

- Platform as a Service
 - Amazon Simple Storage Service (S3)
 - Microsoft Azure
 - Rackspace
- Storage as a Service
 - Dropbox for Teams
 - Box
 - Google Drive (Apps for Business)
 - Symantec Backup Exec.cloud

Environmental Setup

- Accounts
- Sub Accounts
- Dummy Data
- Waiting
- Scripted Communication
- Incident
- Contact

Incident

- Deletion
- Modification
- Support Methods
- Script
- Documentation

Providers and Results

Amazon Simple Storage Service

- **Setup**
 - Administrator console
 - Uploaded files using Web GUI
 - Scripted the syncing between Dropbox to S3 bucket
- **Incident**
 - Accessed administrator console from different IP addresses
 - Deletion and modification
- **Results**
 - Instant support with the right plan
 - Amazon cannot recover objects, once they are deleted they are gone
 - Amazon does not hold copies of data after a delete call has been made. They are purged
 - Logging + multi factor authentication + rotating credentials

Microsoft Azure

- **Setup**
 - Purchased developer support plan that promises <2h response and 3 calls/month
 - Used a third party program: Azure Storage Explorer 4
 - Files are stored as database blob objects
 - Primary access keys and secondary access key
- **Incident**
 - Deleted bobs using primary access key
 - Modified blobs using secondary access key
 - Access storage bucket using different IP addresses
- **Results**
 - No option to create storage related ticket
 - Support call
 - 24 hours till resolution
 - Response: Recommended community support forums

Rackspace

- **Setup**
 - Upload services are available directly through the WebGUI
 - Needed to upload files greater than 2GB through FTP client
- **Incident**
 - Deletion and Modification
- **Results**
 - Could not restore deleted or modified data
 - Network redundancy
 - Clients expected to backup their own data
 - Support: 2 hour response
 - Recovery is unsupported

PaaS Summary

- Amazon
 - Bandwidth applications
 - Scalability
 - Backup solution, not primary storage
 - Strong encryption/authentication.
 - Live chat
- Microsoft Azure
 - Geo replication
 - Ease of use
 - Limited ticketing support
 - 90 day trial
- Rackspace
 - 100% network uptime. 99% storage uptime.
 - Focused on network uptime rather than storage

Dropbox for Teams

- **Setup**
 - Primary administrator
 - Secondary administrator
 - Setup multiple login accounts
- **Incident**
 - Deletion and modification
 - Different IP addresses
- **Results**
 - Contact form
 - 2 hour response
 - Able to recover all files
 - Unable to view changes
 - Packrat
 - Detailed logs
 - Limit use of the primary administrator account

Box

- **Setup**
 - Synced account services with Dropbox
 - Uploaded files using the web GUI
 - Also used Box's FTP client
- **Incident**
 - Deletion and modification
 - Different IP addresses
- **Results**
 - Asked user to identify they were the account owner
 - Require explicit permission to access your data
 - Restored deleted and modified data
 - 6 hour response for deleted files
 - 3-5 days response for modified files

Google Drive (Apps for Business)

- **Setup**
 - Multiple email addresses created per user
 - Installed Google Drive
- **Incident**
 - Administrator modified a file using desktop application
 - Deleted a few files using two different users
 - Renamed a file using different user
- **Results**
 - Support call
 - 24 hours until resolution
 - Able to recover all the files
 - Able to tell modification

Symantec Backup Exec.cloud

- **Setup**
 - Backup service
 - Created a virtual machine to store data and back it up
 - Installed Symantec.cloud on the virtual machine
- **Incident**
 - Attacked using European virtual machine
 - Deletion and modification
- **Results**
 - 24/7 monitoring by operations center
 - Deleted data is indestructible for up to 90 days
 - Able to track IP address to our Europe based machine

Storage as a Service Summary

- **Dropbox**
 - Fast 2 hour resolution. Full recovery.
 - Packrat
 - Ease of use
 - Detailed logs

- **Symantec Exec.cloud**
 - 24/7 phone prompt phone support
 - Able to recovery data and track down attacker
 - Security centered
 - Strictly for backup

Prior Work in Cloud Incident Response

- CGI's steps for working with your cloud provider in event of a security breach
 - Who do you contact?
 - How will your provider shut down if required?
 - How will they segregate and protect data?
 - How will they conduct forensics to isolate the breach

<http://www.cgi.com/en/blog/cloud/cloud-incident-management>

Conclusion

- Familiarize yourself with Cloud Offerings (and limitations!)
- Footprint vs. Service (Bigger isn't always better)
- Migration to the Cloud
- Make sure you have a policy and a way to enforce it
- Planning, Implementation, Reporting, Tracking

Thank You