MOVING INTO THE CLOUD

Ryan Draughn
Gentle Reminder:
Risk of Onsite Data during Disasters

Loss of Investment
https://www.youtube.com/watch?v=1UXHCf9b9g8

Loss of Data
https://www.youtube.com/watch?v=8lLI7qfREJ4
Common Premise Based IT Environment

Expensive in time and resources to install and maintain!

- Expensive hardware with typical 3 - 4 year refresh cycles.
- Reoccurring software license fees.
- Insufficient quantity of IT staff; Skills often not specialized.
- Lacks adequate backups & security.
- Slow restoral of critical business processes after a disaster.
- Environmental (HVAC) costs and may need to adhere to compliancy/regulatory requirements.
Cloud Computing brings Transformational Change

“Cloud Computing - Hosted Desktop - SaaS – IaaS”

Reliable & Secure Data Center
What in the world is Cloud Computing?
Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand.

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers that may be located far from the user—ranging in distance from across a city to across the world.

Leading Cloud Providers

• Provide massive economies of scale to drive down data storage costs.
• Many have developed **PRIVATE** cloud offerings that:
  • Enable data to not be co-mingled with other organizations.
  • Meets individual customer demands for retrieval practices.
  • Adheres to specialized compliance or regulatory demands (PII, HIPAA, PCI)
  • Ensure storage inside of continental US.
• Allow for specialized service providers to develop software platforms built on their data storage foundation.
Types of Clouds

Private Clouds
Public Clouds
Hybrid Clouds
Public Clouds

A public cloud is one in which the services and infrastructure are provided off-site over the Internet. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds.

Ex. Gmail, Dropbox, SaaS Applications

Private Clouds

A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings.

Good when data privacy and security are crucial.

Hybrid Clouds

A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud, you keep each aspect at your business in the most efficient environment possible. The downside is that you have to keep track of multiple different security platforms and ensure that all aspects of your business can communicate with each other.

Your company wants to use a SaaS application but is concerned about security. Your SaaS vendor can create a private cloud just for your company inside their firewall.

Examples of Cloud Services

- Web Site Hosting
- Email
- Phone Systems
- Hosted Desktop
Delivery Models

- **Premise Based**
  - You buy the servers
  - You buy the desktops
  - You buy all of the network equipment
  - You buy and maintain all the licenses

- You pay someone to maintain and support it
- You assume all the risk of ownership.
Delivery Models

- **Cloud or Hosted**
  - **Vendor provides** the servers & hardware.
  - **Vendor supports** software platform.
  - **Vendor maintains** environment 24x7X365.
  - **Vendor assumes** risk of ownership.
  - Little to no up-front capital cost.
  - Scale up/down much more quickly (in many cases monthly)
Statistics

88% Organizations using the public cloud in some capacity.

82% Businesses currently using a hybrid cloud strategy.

74% Companies who believe using a hybrid cloud will grow their business.

https://www.microsoft.com/en-us/cloud-platform/hybrid-cloud
"Growth of public cloud is supported by the fact that organizations are saving 14 percent of their budgets as an outcome of public cloud adoption, according to Gartner's 2015 cloud adoption survey," said Sid Nag, research director at Gartner.
Why Should YOU Care?

- For some, it can
  - Be more cost effective
  - Provide a more scalable solution
  - Require A LOT less up-front capital
  - Be easier to deploy
  - Offer more functionality
  - Provide a much more cost effective DR solution
Moving Into The Cloud

Implementation Considerations
Why is moving to Cloud Computing challenging?

- MIS-Information: Business managers not getting GOOD information
  - Marketing materials are gimmicky and misleading.
  - Business managers recognize benefit but don’t understand all the dynamics.
- Most IT professionals see cloud services as extremely threatening to their job and value they contribute to the organization.
- Cloud service providers are selling services; they aren't ones you should get educated from
- Security concerns or paranoia?

- Organization may not be ready to handle the flexibility that cloud computing provides. Will personnel policies need to change?
Change in Culture and Change in Business Procedures

• Change from CAPEX model to OPEX financial model
  • IT infrastructure no longer purchased as capital expenses and depreciated over its lifecycle.
  • Instead, IT infrastructure paid as operating expense like a utility.

• Shift of some “controls” and “administration” of IT equipment
  • Outsourced vs. dedicated IT staff to perform these duties

• Traditional IT duties shift from PC/network technicians to service managers. Or said differently, IT will shift from being the “mechanics” to the “process improvers” or “service innovators”.
Things You Need to Know

• Your IT is More Complex Than You Think.
• Most organizations do not have a full and robust inventory of data.
• Some applications and processes are temperamental in hosted environments (Scanning, Printing, etc.).
• Cloud will be blamed for everything. Stay committed.
• Plan for culture impact. Enhanced accessibility is immediate.
• Transition costs are hard to predict.
NCLM Status

Cloud Experience
Background/Status at NCLM

• Moved to Private Cloud Offering in December ’12.
• Utilize private cloud offering from VC3, Inc.
• Preceded by SA-Lite Managed Services contract in January ’12.
• Virtualized staff’s desktop environment (approx. 80 seats)
• Hosted Exchange, Anti-SPAM, AV, File/Print Services.
• Moved application servers running insurance claims system (iVOS), Policy mgmt. (Navrisk), document mgmt. (Laserfiche), Finance (Navision), Association Mgmt. System (CRM).
Background/Status at NCLM (Cont.)

• Moved SharePoint (Intranet and Internet)
  • NCLM.org and other websites
• Outsource helpdesk operations (24x7x365)
• Minimal server/network hardware exists onsite
• Change to 64-bit architecture
• Dual monitors for all thin client staff (around 80% of organization)
• Staff embraced change
Financial Component – Former Budget - 2012

Annual Software Cost Highlights

• Microsoft Enterprise Agreement
  • SQL Server, Office, Exchange, SharePoint, CALs
• Symantec Anti-Virus
• MailFoundry Anti-Spam
• Network monitoring tools
• Ticketing system software
• Total: $33,818/annual
Financial Component – Former Budget -2012

Annual Datacenter Cost Highlights

• Storage Area Network (SAN)
• VMWARE Licenses
• ESX Server Environment
• Server Licenses
• Sonicwall NSA and SSL VPN

Total – $43,600/year

 Doesn’t include HVAC costs and RISK of ownership
Since 2012, equivalent IT cost outlay consistently $131,000/yr.

Roughly $40,000 in savings factoring in costs of user hardware.

**Standard Applications**
- Microsoft Office Standard Edition
  - Word, Excel, PowerPoint, Outlook, OneNote...
- Microsoft Exchange Email

**Storage**
- Individual and shared storage for all users
Provider handles..

**Backups**
- Nightly backups
- 30 days of Nightly Backups retention
- Monthly and annual archives

**Security**
- SPAM filtering
- End-point Anti-Virus for devices
And provides..

- **24x7** Service Desk
- Server and Network
  - Administration
  - Patch Management
- **Remote and Onsite Support**
- Software application support
- Patch management for supported software
- **User Satisfaction** tracking

**Hardware**
- Thin client, keyboard, mouse and monitor; All-in-one unit

**Reports and Documents**
- IT Documentation
- IT Performance Report
- Best Practices and Policies Library
The Challenges faced..

- Change in culture: Adopting processes from outside firm
  - Ticketing system, storage quotas, billed for usage, etc.

- Staff lost individual preferences
  - Windows Search/Desktop features

- Oversight of IT operations changed
  - Managing dynamics between IT support staff
  - Re-organization of IT Staff
  - Loss of in-house technical skills over time

- IT under a microscope – Cloud commitment
  - Printing
  - Scanning
  - Sound volume
  - New procedures/change
More Challenges..

- Had to abandon/re-work contracts or relationships with existing partners.
- Cloud provider contract negotiations were dicey.
- IT staff morale – staying committed.
- Equipment or provider loyalty changed.
- Devoted time to training; paid huge benefits.
- Staff wide conversation to set expectations.
  - Staff did not everything they heard.
    (but had to say it anyway)
  - Benefits far outweighed the disadvantages.
Brave New World – The Benefits!

- Organization sees IT in new positive light - Empowerment vs. Service based
  - Focus on enhancements/projects instead of putting out fires
  - CIO - Organizational leader versus IT leader
- Less servers – good exercise to condense VMs that were needed
- Disaster Recovery/COOP plan more flexible and easier to implement
- Enhances staff’s capabilities – Remote work environment, changing work/life balance, generational workforce embraces
- Less pressure on BYOD
- Simplified budgeting
  - Monthly cost per employee
  - Elimination of hardware capital investment
- Monitoring of apps by team of engineers
  - Example of Claims app improvement
  - Proactive monitoring
  - Patches/updates on OUR schedule
Costs

- ROI calculations - factor in IT staff time
  - Managed services produced **substantial savings**: Approximately 25-25%
  - Private cloud service move **more costly in year 1**: Approximately 5% higher
    - Software licenses had to be converted to TLP or required pro versions
  - Estimated net – neutral savings in year two and beyond
  - Hard to calculate efficiencies gained in IT NOT managing hardware but offering process and business improvements

- Hard to calculate overall staff productivity gain by offering more flexible work options, less downtime, faster application response time, new application access options.
Ownership of Data

All data provided by Client Company to Service Provider pursuant to the Agreement is and shall remain the sole property of Client Company and Client Company reserves all right, title and interest (including all intellectual property and proprietary rights) in and to such data.
Access to Data

At its sole discretion, Client Company retains the right to access and retrieve data provided by Client Company that is stored on Service Provider’s infrastructure. This includes physical access to data as well as the right to request data be retrieved by Client Company. The Client Company will give Service Provider advanced notification of 15 days for data access or retrieval.
Data Disclosure to Third Parties

Service Provider will not receive, transmit or otherwise deliver any data provided by Client Company outside of the continental United States, nor will Service Provider transmit or otherwise deliver any such data to any third party (except for Client Company’s employees) without Client Company’s prior written consent.
Disposition of Data Upon Agreement Termination

Upon termination of the Agreement, Service Provider shall, at the option of the Client Company, either return all the data provided by Client Company and any copies thereof to the Client Company, or destroy all the data provided by Client Company and any copies thereof and certify to Client Company that it has done so. Service Provider shall perform its obligations under this paragraph in accordance with the selected option of Client Company within thirty (30) days after Service Provider is notified of the option selected. If Client Company elects that data provided by it be returned, then Service Provider shall make available to Client Company for a complete and secure (i.e. encrypted and appropriately authenticated) download file of Client Company’s data in its native format. The Client Company may optionally request that data be physically returned on hard drives or other physical media. Service Provider warrants that upon request of Client Company, it will submit its data processing facilities for an audit of the measurers described herein.
Data Breaches

Service Provider shall report, either orally or in writing, to Client Company any use or disclosure of data provided by Client Company not authorized by the Agreement or in writing by the Client Company, including any reasonable belief that an unauthorized individual has accessed such data. Service Provider shall make the report to Client Company immediately upon discovery of the unauthorized disclosure, but in no event more than two (2) business days after Service Provider reasonably believes there has been an unauthorized use or disclosure. Service Provider’s report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the Client Company’s data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Service Provider has done or shall do to mitigate any detrimental effect of the unauthorized use or disclosure, and (v) what corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure. Service Provider shall provide such documentation, including a written report, as reasonably requested by Client Customer.
Data Storage Location

Service Provider agrees to receive, store and process all data provided by Client Company only in the continental United States.
Deposition in Litigation

Service Provider agrees to be deposed in litigation cases where data administration processes are required. Any costs incurred by service provider in time or resources is the responsibility of the service provider.
How to Protect Yourself

Protecting information in the cloud
Change in Roles/Responsibilities

“For organizations engaged in wholesale cloud migrations, roles and responsibilities will require significant changes—moving from specialized roles, such as server or network managers, to broader roles for integrated service managers.”

“These service managers will be well positioned to steward business risks because their perspective is more comprehensive than that of specialized managers, for example, when making judgments on when to use private- or public-cloud resources.”
“As attractive as cloud environments can be, they also come with new types of risks. Executives are asking whether external providers can protect sensitive data and also ensure compliance with regulations about where certain data can be stored and who can access the data. CIOs are also asking whether building private clouds creates a single point of vulnerability by aggregating many different types of sensitive data onto a single platform.”

“Blanket refusals to make use of private- or public-cloud capabilities leave too much value on the table from savings and improved flexibility.”
A Risk-Management Approach to Exploiting the Cloud

“In many large institutions, information security traditionally has been a control function that used policies limiting what IT managers and end users could do in order to reduce the likelihood of data loss, privacy breaches, or noncompliance with regulations. We believe that IT organizations must now adopt a business-focused risk-management approach that engages business leaders in making trade-offs between the economic gains that cloud solutions promise and the risks they entail.”
Landscape in 2016
Hybrid Clouds & Industry trends
Business usage of SaaS, Hosted and Cloud Solutions becoming commonplace

- Google Docs
- Office365
- Azure/Onedrive
- Amazon Web Services
Hybrid Clouds leading the way

- Former “public cloud” providers offering robust solutions for specific industries concerned with privacy and security.
  - Ex. Microsoft Azure Government Cloud
Compliance is a commitment, not a checkbox

Rochelle M. Eichner  October 3, 2016

With the recent heartbreaking public safety events in New York, New Jersey, North Carolina, Minnesota and other locations around the United States, it was inspiring to have the opportunity for Microsoft to participate in the South Carolina Law Enforcement Division (SLED) User Conference. It included over 700 law enforcement professionals strategizing on how to use technology to enhance their ability to achieve the goal of citizen and officer safety.

One of the primary objectives of law enforcement today is to deploy solutions that connect systems, people, and devices in real-time to improve police response... and implement these solutions in a secure and CJIS compliant manner. Microsoft Government Cloud services give agencies that opportunity. As indicated by South Carolina CJIS Information Security Officer, Bruce Smalley “Agencies can be CJIS compliant using cloud services. Microsoft has raised the bar for providing CJIS compliance attestation for the government cloud.”

In addition, Richard Zak, Director, Microsoft Justice and Public Safety, and I presented, “Delivering a CJIS-Compliant Cloud for US Law Enforcement Agencies”, detailing Microsoft’s commitment to CJIS compliance and law enforcement solutions for officer and court management, pro-active policing, CAD/RMS, and police video. These solutions are widely deployed today in law enforcement in a secure and compliant manner on Microsoft Government Cloud services reducing crime and improving officer safety.

Other cloud providers appear to treat CJIS compliance as a checkbox rather than a commitment. At Microsoft, we are committed to providing solutions that meet the applicable CJIS controls today and in the future. In addition, we extend our commitment to Justice and Public Safety thru to our Digital Crimes Center, Cyber Security Operations Center, Future Patrol Vehicle, and World-wide Justice and Public Safety organization.

For additional implementation information, review the Microsoft CJIS Implementation Guidelines. This document provides guidelines and resources to assist criminal justice entities in implementing and utilizing Microsoft Government Cloud features.

We welcome your comments and suggestions to help us continually improve your Azure Government experience. To stay up to date on all things Azure Government, be sure to subscribe to our RSS feed and to receive emails, click “Subscribe by Email” on the Azure Government Blog. To experience the power of Azure Government for your organization, sign up for an Azure Government Trial.
Major Vendors will continue to push customers to their SaaS offerings

Claims and Policy Management Application Vendors are no exception
Beyond the Cloud

Many industry experts are predicting machine learning, serverless environments, and a focus on data will be the “future” of cloud computing over the next several years.

Eric Schmidt, CEO of Google states, “the amount of innovation we will see in the next five years will exceed all the innovation we’ve seen in all prior years. Schmidt went on to make a few more predictions:

The platform is not the end, it is the bottom. Machine learning is on top and will be the technology that will drive the transformation. NoOps will become mainstream. Serverless architectures will be the next wave of computing.

http://www.forbes.com/sites/mikekavis/2016/03/25/google-provides-a-glimpse-into-the-future-of-cloud-computing/#5b2753f5529f
Questions?