SCHNEIDER DOWNS

Welcome to the Schneider Downs Quarterly Not-for-Profit Breakfast Briefing

Cloud Computing for the 21st Century Not-for-Profit Organization

Presented by:
Christopher R. Debo, Senior Manager, Schneider Downs Technology Advisors
Jason M. Reljac, Manager, Schneider Downs Technology Advisors

Big Thinking. Personal Focus.

SCHNEIDER DOWNS

How does your organization **USE** the cloud?

Understand – Secure – Evaluate

Big Thinking. Personal Focus.

Who we are

- Chris Debo
  - Technology Advisors
  - Columbus Office
  - Technically savvy, security-conscious consultant
- Jason Reljac
  - Technology Advisors
  - Pittsburgh Office
  - Technically savvy, somewhat nerdy consultant
- Patrick Armknecht
  - Technology Advisors
  - Pittsburgh Office
  - Sales guy with accounting background
  - Skipped town on us but provided slides

Combined 40+ years of technology consulting experience in a wide range of industries

Big Thinking. Personal Focus.

Agenda

- Understanding the Cloud
- Securing the Cloud
- The Changing role of IT in the Cloud
- Evaluating the cost/benefit of using the Cloud vs. on premise

Big Thinking. Personal Focus.

Defining the "Cloud"

- **Wikipedia** "a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand."
- **PC Magazine** "A communications network. The word "cloud" often refers to the Internet, and more precisely to some datacenter full of servers that is connected to the Internet."
- **Merriam-Webster** "the practice of storing regularly used computer data on multiple servers that can be accessed through the Internet"

Big Thinking. Personal Focus.

Defining the "Cloud"

- **Investopedia** "Cloud computing is a model for delivering information technology services in which resources are retrieved from the internet through web-based tools and applications, rather than a direct connection to a server."
- **Dictionary.com** "Internet-based computing in which large groups of remote servers are networked so as to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources."
- **National Institute is Standards and Technology** "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources"
- **IBM** "Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources—everything from applications to data centers—over the Internet on a pay-for-use basis."
- **Amazon** ""Cloud Computing", by definition, refers to the on-demand delivery of IT resources and applications via the Internet with pay-as-you-go pricing."
- **Gartner** "...as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies."

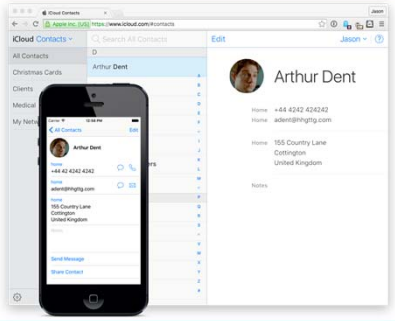
Big Thinking. Personal Focus.

My definition

A service, just like electricity, cable or water, that you or your organization subscribes to that puts data of yours in someone else's possession while making it easy to access and forget about.

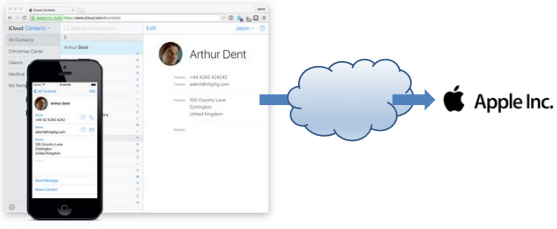
Big Thinking. Personal Focus.

This is cloud



Big Thinking. Personal Focus.

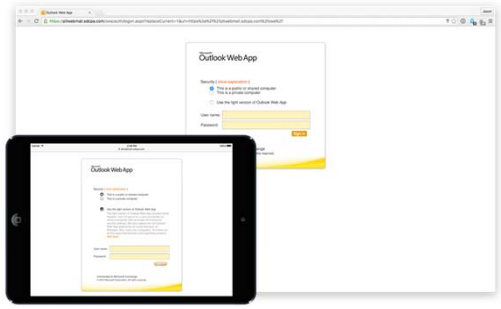
Why?



I work for Schneider Downs but with iCloud my contacts are stored on Apple's servers.

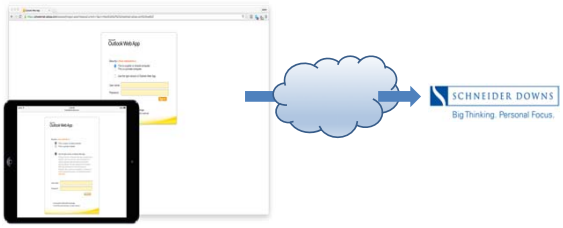
Big Thinking. Personal Focus.

This is NOT Cloud



Big Thinking. Personal Focus.

This is NOT Cloud



I work for Schneider Downs and with Outlook web access I am accessing my Schneider Downs email over the internet but am accessing a server AT Schneider Downs.

Big Thinking. Personal Focus.

What makes up the Cloud

Documents
- Amazon Cloud Drive
- Apple iCloud
- Dropbox
- Google Drive
- Microsoft OneDrive

Communications
- Conference calls
- Email
- Global Connect
- Instant messaging
- Voice mail

Audio/Video
- Amazon Music Player
- iTunes
- Netflix
- YouTube
- Vimeo

Productivity
- Apple iCloud
- Google Docs
- Lucidchart
- Microsoft Office 365
- Zoho Docs

Enterprise Servers
- Amazon AWS
- Local providers
- Microsoft Azure
- Rackspace Cloud

ERP
- Microsoft
- Oracle
- SAP
- Many others…

Enterprise Applications
- Human resources
- Payroll processing
- Video monitoring
- Time and expense entry

Big Thinking. Personal Focus.

Cloud ≠ Data Center

But, you are keeping track of your data center, right?

Cloud ≠ Disaster Recovery

It's a piece of the puzzle

Easy Cloud Moves

- Email
  - Usually eliminates
    - Servers
    - SPAM
  - Generally adds
    - Enhanced remote access
  - Easy and cost-effective
  - IT usually hates email servers anyway
  - Can't forget about downtime

Common Cloud Moves

- Office productivity applications
  - Heavy macro users?
  - Tied to other enterprise applications?
- Enterprise applications
  - Time & expense tracking
- Human resource management
- Payroll processing
  - Can eliminate printed pay stubs & tax filing
  - Can add open enrollment, self-service

Big Thinking. Personal Focus.

Involved Cloud Moves

- Accounting
  - Lots of moving parts
- ERP
  - Lots and lots of moving parts
- Manufacturing
  - Inventory
  - Shop floor

Big Thinking. Personal Focus.

Cloud – Acronym Soup

- DRP
- HIPAA
- ISO
- PCI DSS
- SOC 1 & 2
- SOX
- SSL 64/128/256/512

Big Thinking. Personal Focus.

Ask & Understand

No guessing ;-)

Cloud – Acronym Soup

- DRP - Disaster Recovery plan
- HIPAA - Health Insurance Portability and Accountability Act
- ISO - International Organization for Standardization
- PCI DSS - Payment Card Industry Data Security Standard
- SOC 1 & 2 - Report on Controls at a Service Organization
- SOX – Sarbanes-Oxley
- 64/128/256/512 – Levels of SSL encryption
- SSL – Secure Sockets Layer

Big Thinking. Personal Focus.

It's not just you that needs to understand...

Your vendors do as well

If they don't understand or seem confused it might be time to re-evaluate them as a vendor

Why Should I Care?

Big Thinking. Personal Focus.

Why Should I Care?

Big Thinking. Personal Focus.

Why Should I Care?

Big Thinking. Personal Focus.

Why Should I Care?


Los Angeles Times

LOCAL U.S. WORLD BUSINESS SPORTS ENTERTAINMENT HEALTH LIVING TRAVEL OPINION

MONEY & CO. TECHNOLOGY HIGHWAY 1 COMPANY TOWN PERSONAL FINANCE JOBS REAL ESTATE CARS

YOU ARE HERE: LAT Home → Collections → User Information

Ads by Google

EPICOR

Discover ERP built around you

Microsoft employees hacked; Azure cloud service inaccessible

February 22, 2013 | By Salvador Rodriguez

Email Share +1 Tweet

It was a rough Friday for Microsoft, which suffered a major

Big Thinking. Personal Focus.

Cloud Computing Risks - Technical

Threat	Description	Risk Mitigation / Control Strategy
Vulnerable access management (infrastructure and application).	Information assets could be accessed by unauthorized entities due to faulty or vulnerable access management measures or processes. This could result from a forgery/theft of legitimate credentials or a common technical practice (e.g., administrator permissions override).	• Contractual agreements to clarify who is allowed access. • Review identity access management controls of the cloud services provider (CSP), SOC 1, SOC2. • Where possible use your own identity access management controls and systems and not the CSP's.

Big Thinking. Personal Focus.

Cloud Computing Risks - Technical

Threat	Description	Risk Mitigation / Control Strategy
Data visible to other tenants when resources are allocated dynamically.	This refers to data that have been stored in memory space or disk space that can be recovered by other entities sharing the cloud by using forensics techniques.	• Contractual agreements to clarify who is allowed access • Encrypt all sensitive assets and data • Request the CSP's technical specs for wiping data from systems • Use a private cloud model with no multitenancy

Big Thinking. Personal Focus.

Cloud Computing Risks - Technical

Threat	Description	Risk Mitigation / Control Strategy
Multitenancy visibility. Due to the nature of multitenancy, some assets (e.g., routing tables, media access controls [MAC] addresses, internal IP addresses, local area network [LAN] traffic) can be visible to other entities in the same cloud.	Malicious entities in the cloud could take advantage of the information; for example, by utilizing shared routing tables to map the internal network topology of an organization, preparing the way for an internal attack.	• Contractual agreements to clarify who is allowed access • Request a SOC 1, SOC2 report. • Use a private cloud model with no multitenancy

Big Thinking. Personal Focus.

Cloud Computing Risks - Technical

Threat	Description	Risk Mitigation / Control Strategy
Application vulnerability attacks	Due to the nature of SaaS, the applications offered by a CSP are more broadly exposed. Because they can be the target of massive and elaborate application attacks, additional security measures (besides standard network firewalls) are required to protect them.	• Request that the CSP implements application firewalls, antivirus and antimalware tools. • SaaS developed using OWASP standards. • SLAs or SOC reports must contain detailed specifications about vulnerability testing, classification and actions taken according to the severity level.

Big Thinking. Personal Focus.

Cloud Computing Risks - Technical

Threat	Description	Risk Mitigation / Control Strategy
Collateral damage	The organization can be affected by issues involving other entities sharing the cloud. For example, DDoS attacks affecting another entity in the cloud can leave the organization without access to business applications (for SaaS models) or extra computing resources to handle peak loads (for IaaS models).	• Ask the CSP to include the organization in its incident management process that deals with notification. • Ensure the contracted capacity is always available and cannot be directed to other tenants without approval. • Use a private cloud model with no multitenancy.

Big Thinking. Personal Focus.

Cloud Computing Risks - Regulatory

Threat	Description	Risk Mitigation / Control Strategy
Asset ownership	Any asset (data, application or process) migrated to a CSP could be legally owned by the CSP based on contract terms. Thus, the organization can lose sensitive data or have data disclosed because the organization is no longer the sole legal owner of the asset. In the event of contract termination, the organization could even be subject (by contract) to pay fees to retrieve its own assets.	• Include terms in the contract with the CSP that ensure that the organization remains the sole legal owner of any asset migrated to the CSP. • Encrypt all sensitive assets being migrated to the CSP prior to the migration to prevent disclosure and ensure proper key management is in place.

Big Thinking. Personal Focus.

Cloud Computing Risks - Regulatory

Threat	Description	Risk Mitigation / Control Strategy
Asset disposal	In the event of contract termination, to prevent disclosure of the organization's assets, those assets should be removed from the cloud using tools and processes commensurate to data classification; forensic tools may be necessary to remove sensitive data (or other tools that ensure a complete wipeout).	• Request CSP's technical specifications and controls that ensure that data are properly wiped and backup media are destroyed when requested. • Include terms in the contract that require, upon contract expiration or any event ending the contract, a mandatory data wipe carried out under the organization's review.

Big Thinking. Personal Focus.

Cloud Computing Risks - Regulatory

Threat	Description	Risk Mitigation / Control Strategy
Asset Location	Information assets (i.e. data) are subject to the regulations of the country where they are stored or processed. A CSP may, without notification, migrate information assets to countries where regulations are less restrictive or their transmission is prohibited. Unauthorized entities that cannot have access to assets in one country may be able to obtain legal access in another country. Conversely, if assets are moved to countries with stricter regulations, the organization can be subject to legal actions and fines for noncompliance.	• Request the CSP's list of infrastructure locations and verify that regulations in those locations are aligned with your organization's requirements. • Include terms in the service contract to restrict the moving of organizational assets to only those areas known to be compliant with the organization's own regulatory concerns. • To prevent disclosure, encrypt any asset prior to migration to the CSP, and ensure proper key management is in place.

Big Thinking. Personal Focus.

Cloud Computing Risks - Governance

Threat	Description	Risk Mitigation / Control Strategy
Physical security on all premises where data/applications are stored	Physical security is required in any infrastructure. When the organization migrates assets to a cloud infrastructure, those assets are still subject to the corporate security policy, but they can also be physically accessed by the CSP's staff, which is subject to the CSP's security policy. There could be a gap between the security measures provided by the CSP and the requirements of the organization .	• Request the CSP's physical security policy. • CSP's independent security reviews or certification reports (e.g., SOC1, SOC 2 report, SOX, PCI DSS, HIPAA, ISO, etc.). • Contract language that requires the CSP to be aligned with the organization's security policy. • CSP's disaster recovery plans and ensure that they contain the necessary countermeasures to protect physical assets during and after a disaster.

Big Thinking. Personal Focus.

Cloud Computing Risks - Governance

Threat	Description	Risk Mitigation / Control Strategy
Visibility of the security measures put in place by the CSP	The cloud is similar to any infrastructure in that security measures (technology and processes) should be in place to prevent security attacks. The security measures provided by the CSP should be aligned with the requirements of the organization, including management of security incidents.	• CSP's independent security reviews or certification reports (e.g., SOC1, SOC 2 report, SOX, PCI DSS, HIPAA, ISO, etc.). • Contract language that requires the CSP to provide regular reporting on security (incident reports, intrusion detection system [IDS]/intrusion prevention system [IPS] logs, etc.). • Request the CSP's security incident management process to be applied to the organization's assets and ensure that it is aligned with the organization's own security policy.

Big Thinking. Personal Focus.

Cloud Computing Risks - Governance

Threat	Description	Risk Mitigation / Control Strategy
Media management	Data media must be disposed in a secure way to avoid data leakage and disclosure. Data wipeout procedures must ensure data cannot be reproduced when data media is designated for recycle or disposal. Controls should be in place during transportation (encryption and physical security). This should be specified in the CSP security policy and contract SLA.	• Request the CSP's process and techniques in place for data media disposal and evaluate whether they meet the requirements of the organization. • Include in the contract language that requires the CSP to comply with the organization's security policy.

Big Thinking. Personal Focus.

Cloud Computing Risks - Governance

Threat	Description	Risk Mitigation / Control Strategy
Secure software SDLC	When using SaaS services, the organization must be sure that the applications will meet its security requirements. This will reduce the risk of theft, disclosure and unavailability.	• Request the CSP's details about the software SDLC policy and procedures in place and ensure that the security measures introduced into the design are compliant with the requirements of the organization. • CSP's independent security reviews or certification reports (e.g., SOC1, SOC 2 report, SOX, PCI DSS, HIPAA, ISO, etc.).

Big Thinking. Personal Focus.

Cloud Computing Risks - Governance

Threat	Description	Risk Mitigation / Control Strategy
Service termination issues	Currently, there is very little available in terms of tools, procedures or other offerings to facilitate data or service portability from CSP to CSP. This can make it very difficult for the organization to migrate from one CSP to another or to bring services back in-house. It can also result in serious business disruption or failure should the CSP go bankrupt, face legal action, or be the potential target for an acquisition.	• Ensure by contract or SLA with the CSP an exit strategy that specifies the terms that should trigger the retrieval of the organization's assets in the time frame required by the enterprise. • Implement a DRP, taking into account the possibility of complete CSP disruption.

Big Thinking. Personal Focus.

Cloud Computing Risks - Governance

Threat	Description	Risk Mitigation / Control Strategy
Support for audit and forensic investigations	Security audits and forensic investigations are vital to the organization to evaluate the security measures of the CSP. Performing these actions requires extensive access to the CSP's infrastructure and monitoring capabilities, which are often shared with other CSP's customers. The organization should have the permission of the CSP to perform regular audits and to have access to forensic data without violating the contractual obligations of the CSP to other customers.	• Request the CSP the right to audit as part of the contract or SLA. If this is not possible, request security audit reports by trusted third parties. • Request that the CSP provide appropriate and timely support (logs, traces, hard disk images, etc.) for forensic analysis as part of the contract or SLA. If this is not possible, request to authorize trusted third parties to perform forensic analysis when necessary.

Big Thinking. Personal Focus.

Next Steps in My Organization

- ✓ Identify and list out all cloud service providers
  - ✓ **Involve various departments, chances are there are cloud services providers you may not know about!**
- ✓ Identify the service model for each
- ✓ Identify the deployment model for each
- ✓ Consider risks noted for each cloud service provider
- ✓ Identify controls in place to mitigate the risks
- ✓ Setup a plan to test the effectiveness of the controls in place

Big Thinking. Personal Focus.

The Changing Role of IT in the Cloud

Big Thinking. Personal Focus.

Role of IT for on Premise Solutions

Typical responsibilities of IT resources supporting on-premise applications includes:

- o System administration
- o Network administration
- o Web administration
- o Database administration
- o Security/control administration
- o Backup administration
- o End user support/help desk

Big Thinking. Personal Focus.

Role of IT for Cloud Solutions

Typical responsibilities of IT resources supporting cloud applications includes:

- Data integration
- Service/vendor management
- Project and product management
- Security, compliance, and risk management
- End user support/help desk

Big Thinking. Personal Focus.

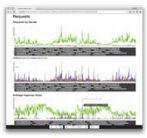
Expectations of IT - Data Integration

- Identify integration requirements across business units.
- Choose the tools/method of integration (e.g., APIs).
- Determine and implement the practices/policies that will be followed for integrating data.
  - These may differ depending upon whether you are integrating with on-premise or other cloud solutions.
- Migrate legacy data to cloud based solutions.
- Provide ongoing support and modifications to data integrations.

Big Thinking. Personal Focus.

Expectations of IT - Service Management

- Prepare costing projections and product capability comparisons.
- Review cloud provider's Service Level Agreements (SLAs) to ensure they align with the needs of your organization.
- Monitor the vendors performance against SLAs.
  - Performance
  - Remediation
  - Availability
  - Disaster recovery



Big Thinking. Personal Focus.

Expectations of IT – Project/Product Management

- Serve as a liaison between end-users and cloud provider to ensure that end-users needs are being met.
- Ensure that the solutions being deployed have been thoroughly vetted and implemented to meet the needs of the organization.
- Fine-tune the application for optimal performance
- Prepare/execute transition plans.

Big Thinking. Personal Focus.

Expectations of IT – Security, Compliance and Risk Management

- Define and apply policies for:
  - Secure authentication;
  - Data encryption, and
  - Access control

  Confirm that the cloud solution chosen complies with the aforementioned policies.
- Identify the jurisdictions in which the cloud provider operates and ensure the legal requirements of those jurisdictions align with your policies.
- Ensure data and information is properly protected.
- Enforce privacy policies.

Big Thinking. Personal Focus.

Expectations of the IT Management in the Cloud

- Be able to communicate the business value of cloud computing to stakeholders.
- Have a clear understanding of the business goals.
- Manage external (vendor) and internal teams.
- Match provider capabilities to company needs.
- Manage, develop and advise IT staff to meet the shifting needs of cloud computing.
- Mitigate company risk by ensuring compliance and protecting data.

Big Thinking. Personal Focus.

Tips for a Successful Transition to the Cloud

- Embrace collaboration as it will be more important than ever.
  - With other departments/business units
  - Cloud vendors
- Obtain an in depth understanding of the business strategy, departmental requirements and operating procedures.
- Identify where savings driven by the cloud can be put to best use and consider the value IT can add to the business.
- Help your IT staff understand the opportunities and challenges the cloud presents and invest in helping them meet those challenges.

Big Thinking. Personal Focus.

Cloud or On Premise?

Vs.

Big Thinking. Personal Focus. 50

Cloud vs. On Premise: 4 Important Questions

1. What deployment options are available (cloud, on-premise or both)?
2. What's the vendor's commitment to developing and supporting these deployment options in the future?
3. Are there any technological barriers to consider?
   - e.g., bandwidth/internet pipe restrictions
4. What is my **Total Cost of Ownership (TCO)?**

Big Thinking. Personal Focus.

IT Total Cost of Ownership Defined

Total Cost of Ownership (TCO) as defined by Gartner:

"A comprehensive assessment of information technology (IT) or other costs across enterprise boundaries over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses and the opportunity cost of downtime, training and other productivity losses."

Big Thinking. Personal Focus.

What's Included in an IT TCO Calculation

- License fee (on premise solutions)
- Subscription Fee (cloud solutions)
- Installation (on premise solutions)
- Training (both)
- Setup (both)

Big Thinking. Personal Focus.

What's Included in an IT TCO Calc. Cont.

- Customization (usually available in on premise solutions often restricted in cloud solutions)
- Integration (both)

- Annual Maintenance (on premise solutions)
- Support Costs (Typically just for on premise solutions as it is included in cloud subscription fees)

Big Thinking. Personal Focus.

What's Included in an IT TCO Calc. Cont.

- Hardware (on premise solutions)
- **Other Costs (both)**
  - Other costs are the items most frequently left out of TCO calculations.

Note: TCO calculations should be modelled over several years. The most common modelling cycles for technology investments are 5, 8 and 10 years.

Big Thinking. Personal Focus.

Often Missed "Other Costs" - On Premise

- Electricity
  - Servers
  - Cooling
- Hardware replacement cost (know your lifecycle)
  - Servers, switches, hubs, routers, etc.
- Operating/database software upgrade cost
  - Operating system (Windows 20xx), database (SQL 20xx), etc.
- Time of setting up infrastructure to support the application

Big Thinking. Personal Focus.

Often Missed "Other Costs" - On Premise

- Antivirus software
- Backup software or cloud backup service
- Cost of internal or external IT resources
  - Maintenance/updates/patches for server, network, databases, etc.
  - Outsourced cost of application upgrades
- Remote access licensing
  - Employees typically need to leverage Citrix or VPN to access on the application from remote locations

Big Thinking. Personal Focus.

Often Missed "Other Costs" - Cloud

- Bandwidth
  - Connection speeds from your office may be limited. Cost to improve can be hefty.
  - Outbound bandwidth from cloud servers often have a limit and then additional fees are charged.
- Downtime – What's the cost of not being able to access your application?
- Integration Costs
  - On premise application
  - Other Cloud applications

Big Thinking. Personal Focus.

Often Missed "Other Costs" - Cloud

- Separation or exit costs – a.k.a., the cost associated with leaving a cloud solution
- Cost of internal or external IT resources
  - Vendor management
  - Security, compliance & risk

A misperception about the cloud is that there are no internal IT costs. Although fees may be reduced, they will not be completely eliminated.

Big Thinking. Personal Focus.

TCO Example – **On Premise** Year 1

Licensing Cost	$XX,XXX
Installation	$ X,XXX
Implementation, Training & Setup Cost	$ X,XXX
Customization and Integration Cost	$ X,XXX
Data Migration Costs	$ X,XXX
Maintenance & Support	$XX,XXX
Hardware Costs:	$ X,XXX
(Servers, PCs, Networking Infrastructure)	
Other Costs:	
In-house IT	$ X,XXX
Backup	$ X,XXX
Antivirus	$ X,XXX
Electricity	$ X,XXX

Big Thinking. Personal Focus.

TCO Example – Cloud Year 1

~~Licensing~~ Subscription Cost	$XX,XXX
~~Installation~~	~~$ X,XXX~~
Implementation, Training & Setup Cost	$ X,XXX
Customization and Integration Cost	$ X,XXX
Data Migration Costs	$ X,XXX
~~Maintenance & Support~~	~~$XX,XXX~~
~~Hardware Costs:~~	~~$ X,XXX~~
Other Costs:	
In-house IT	$ X,XXX
~~Backup~~	~~$ X,XXX~~
~~Antivirus~~	~~$ X,XXX~~
~~Electricity~~	~~$ X,XXX~~
Bandwidth (Maybe)	$ X,XXX
Downtime	$ X,XXX

Big Thinking. Personal Focus.

TCO Example – Years 2 through 4

On Premise		Cloud	
Maintenance & Support	$XX,XXX	Subscription Cost	$XX,XXX
Consulting/Upgrade	$ X,XXX	Other Costs:	
Other Costs:		In-house IT	$ X,XXX
In-house IT	$ X,XXX	Downtime	$ X,XXX
Backup	$ X,XXX		
Antivirus	$ X,XXX		
Electricity	$ X,XXX		

Big Thinking. Personal Focus.

TCO Example – Year 5

On Premise		Cloud	
Maintenance & Support	$XX,XXX	Subscription Cost	$XX,XXX
Consulting/Upgrade	$ X,XXX	Other Costs:	
Hardware	$ X,XXX	In-house IT	$ X,XXX
Operating/database upgrade	$ X,XXX	Downtime	$ X,XXX
Other Costs:			
In-house IT	$ X,XXX		
Backup	$ X,XXX		
Antivirus	$ X,XXX		
Electricity	$ X,XXX		

Note: This model assumes that the lifecycle for replacing hardware and upgrading the operating system & database software is every 5 years.

Big Thinking. Personal Focus.

SCHNEIDER DOWNS

Comments/Questions?

SCHNEIDER DOWNS

Thank you for coming!

Save the Date for our next
Not-for-Profit Breakfast Briefing:
June 16, 2016