Cloud Services and Business Process Outsourcing

What security concerns surround Cloud Services and Outsourcing?

Prepared for the Western NY ISACA Conference
April 28 2015
Kevin Wilkins is the Chief Technology Officer (CTO) at iSecure LLC. Mr. Wilkins oversees the implementations of Network Security product portfolios specializing in the heavily regulated environments such as PCI, SOX, HIPPA/HITECH. Mr. Wilkins has been in the IT industry since 1998 and has had extensive operational experience in Network Engineering, Systems Administration, Telecommunications, and Information Security.
Abstract

• Businesses have been outsourcing various processes and services for many years. Recently, IT services and applications have been moved to "The Cloud". What are the benefits and risks in utilizing outside parties vs. direct hires and internal infrastructure? What are some considerations in making a move to The Cloud safely?
Audience

- Corporate/Information Security Officers
- Business Managers
- IT Administrators
What is Outsourcing in general?

• Take a business process - anything really - and pay an outside party to help.

• “Strictly Business” Examples: Accountancy, Legal, Personnel and Hiring.

• “IT” Examples: Voice Communications, WAN Management, Email, Web Hosting, Public DNS, CRM, Data Backups, Data Storage and Accessibility.
Why Outsource?

• Outsourcing allows a company to focus on their core competencies without requiring the specialized IT knowledge and infrastructure be maintained in-house.

• While you specialize in “manufacturing”, or “finance”, an outside party can specialize in the business support services you need.

• Consultants can work on an as-needed basis instead of carrying the expense of a full-time hire.
Why Outsource?

• Outsourcing a business function can introduce better scalability and elastic resources.

• There is an economic advantage in sharing a larger system.

• Capital expense related to equipment purchases and maintenance can be converted to a monthly payment covering exactly what you need.
What is “The Cloud”? 

• “The Cloud” usually applies to the outsourcing of IT Operations.

• “The Cloud” generally means obtaining Data Handling or Application Delivery from an outside party.

• The other common Silos of “Infrastructure” and “People” are often involved. This relates to the 3rd party management of on-site systems and network components.
Is “The Cloud” new?

• Only in name!

• PBX/Telephone functions have been outsourced via Centrex and VOIP. Traditional ISPs have hosted Email, Web Hosting, DNS, etc. for decades.

• There has been a shift to ISPs specializing on Communications Infrastructure while letting others specialize on the Application and Data side.
I'm pretty sure “The Cloud” is new.

• OK, so it is.

• The variety, accessibility, and scalability of IT functions which can be outsourced continues to grow.

• The variety of business operations that can push their Data and Applications to a Hosted environment also grows.
Great, I want it!

Cool, but did you ask your CSO?
Our friendly CISSP says that good security is centered around the following...

- Confidentiality – Is your data private?
- Integrity – Is your data intact, and protected from modification, damage or destruction?
- Availability – Can you use your data or application where and when you need it?
What are some concerns with Outsourcing?

- Other People have access to your Data - how are they held accountable for it?

- This might include Accounting Data, Customer Contacts, Strategic Information, Trade Secrets, and Sensitive Communications.

- This might also include access to your Network and Internal Systems in the case of Managed Services.
What are some concerns with Cloud Service providers?

• Cloud Based data and applications may be globally accessible to remote workers, but also exposed to attack by outside parties.

• Can the Cloud Service send you security logs and reports in regards to access attempts and failures, and notify you in the event of an attack or a breach?
What are some concerns with Cloud Service providers?

• Does your Cloud service support Data Loss Prevention (DLP) functionality?

• What if the data is lost (as in destroyed) or disclosed (stolen or leaked) to unauthorized parties?
What are some concerns with Cloud Service providers?

• The Data and Applications are off-site, which could lead to Accessibility issues if your Internet connections go down.

• What happens if the entire Cloud Service provider were to go out of business?
Data Ownership in The Cloud

• Some Cloud Services claim ownership or usage rights to your data. For example, YouTube will claim rights to repackage, distribute, or sell anything you upload for their own benefit.

• Amazon Web Services explicitly protects your rights to your intellectual property in their EULA.

• What happens to data when an employee buys a Cloud Service for your company, but uses a personal credit card and identity information to set up the account? What happens if this account is used to host Company data, but the employee leaves the Company?
Mobility and BYOD

• As previously mentioned, moving data to Cloud Service can simplify access by remote workers.

• Remote Access can be related to Mobile Access, but that’s a different presentation! And don’t get me started on Bring Your Own Device (BYOD)...

• The relationships of BYOD, Mobile, and Cloud can be discussed during Q/A at the end of this presentation.
Jeez, what else?

• Many cloud providers will limit their liability in the event of downtime, data loss, or compromise.

• The ability to directly manage a service outage is limited. You can call support, but often answers are not forthcoming. This can be frustrating, especially if a critical service is offline.

• The ability to customize may be limited. “It Is What It Is”. You may only see new capabilities as part of the Cloud Service providers’ development roadmap, not your own requirements.
What can be done internally to mitigate security concerns when Outsourcing?

• Maintain a local backup copy of your data.

• Have Business Continuity and Disaster Recovery plans if the Cloud service suffers a serious issue.

• Prepare a Cloud Exit Strategy including a process, hardware / software manifest, and projected costs.
What can be done to secure your data that’s been entrusted to outside parties and accessible via Public Internet?

• Crypto fairy-dust goes a long way. There are 3rd party solutions on the market that can encrypt your data in transit to a Cloud based provider and provide decryption services when the data is retrieved.
What can be done to secure your data that’s been entrusted to outside parties and accessible via Public Internet?

• Some Cloud providers provide encryption of Customer data while in storage and in use, and provide ability for the Customer to control the encryption keys. This provides an assurance that employees of the Cloud provider or other outside parties cannot read your data.
What can be done to secure your data that’s been entrusted to outside parties and accessible via Public Internet?

• Single Sign On (SSO) can tie independent Cloud Provider authentication mechanisms into a single login associated with your Active Directory system. This greatly simplifies password management.

• SSO service providers can also extend the functionality of a Cloud Provider with additional security controls (Time of Day, Geographical ID, DLP, Device Restrictions) and auditing.
How can a relationship with a Cloud-based provider be managed in order to limit risk?

• Consider a requirement that the Cloud Service provider release your data in a common and portable format on demand. Avoid vendor lock-in.

• Easy access to “raw” data may also prove important when dealing with legal and e-discovery issues.

• Ensure that the Cloud Service provider has the required level of compliance and governance for the security of your data.
How can a relationship with a Cloud-based provider be managed in order to limit risk?

• Ensure that the Cloud Service provider has a Business Continuity Plan and Disaster Recovery strategy with stated Service Level Agreements for restoration or customer compensation/remedy.

• Read the EULAs and Contracts very carefully. If the stakes are high, try to negotiate the terms.
How can a relationship with a Cloud-based provider be managed in order to limit risk?

• Depending on the level of exposure, treat Outsourced and Cloud Services providers like any other business partner. Perform as much vetting as you might give an accountant or lawyer.

• Consider a Bonded agreement to ensure proper care and accountability, or verification of an insurance policy to cover potential losses.

• Consider requiring 3rd party audits of a Cloud Service provider’s practices.
A Scary Story...

- Nirvanix, a cloud-storage company, announces a termination of operations. Customers had two weeks to move their data. Uploads were disabled immediately.

- This affects both independent customers as well as strategic partnerships with IBM SmartCloud and other major players such as Dell, HP, and Symantec.

A Scary Story...

- An outside company providing HVAC management services was implicated in the Target breach.

- The HVAC company had been granted excessive access to Target’s network. When their own systems and credentials had been compromised, Target was left vulnerable.

- Do we blame Target, or the HVAC company?
Some thoughts regarding Over-Dependence on Outsourcing

• Outside consultants and managed service providers may not have the same personal investment in an organization versus a full-time employee. To an outsourcing provider, you are just another customer while an employee’s dedication and behavior has a direct impact on himself, his company, and his fellow employees.
Some thoughts regarding Over-Dependence on Outsourcing

• An outside consultant, MSP, or Cloud Service provider might not have the desire or latitude to “go the extra mile”. Contractual agreements might prohibit a 3rd party employee from providing assistance not defined in the SLA without approval from management. This is due to both pricing and liability concerns.
Some thoughts regarding Over-Dependence on Outsourcing

• An over dependence on outsourcing can result in a brain-drain within your own organization. A day might come when you have insufficient technical knowledge within your organization to effectively manage a vendor, understand the service they offer, and deal with integration issues.

• This is compounded when interoperability issues occur between your multiple service providers.
I get it. You hate “The Cloud”.

• No. The Cloud is cool and can make your life easier. But “Cloud Service” is a buzzword and providers make it very easy to launch into. When there are problems, it’s a long way down.

• When properly managed, you can achieve economical access to specialized and scalable services while maintaining operational stability and security of data.
In Summary

• Business Process Outsourcing and use of Cloud Services has proven benefits and is common practice.

• Conduct careful planning regarding how services will be used, how to manage problems, and build policies defining what data is acceptable for use in The Cloud.

• Structure your agreements with Cloud Service partners in such a way that carries assurances of accountability, liability, compliance, ownership, and smooth disengagement when the term of service has ended.
Questions and Answers