Dopkins Information Security Series

Lifting the Fog to See the Cloud

Navigating the complex world of cloud computing can be difficult. It's important to ask the right questions before diluting your control over your data.

Learn about the benefits and challenges that face companies in today's hosted environment and receive valuable takeaways that you can implement immediately.

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Contents

For more information on the services we offer, please visit

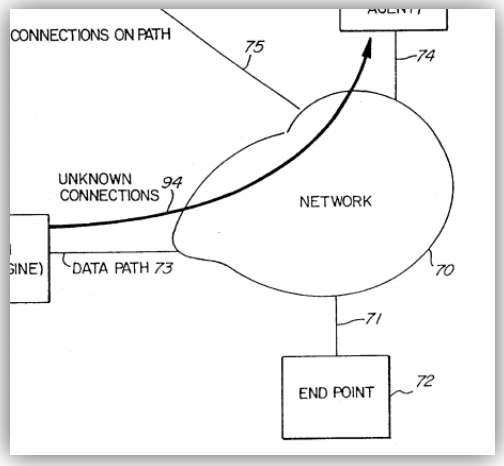
dopkins.com/services

Introduction: Cloud Computing

"*It's in the cloud*." A common expression in today's business jargon that is often misunderstood and misconstrued. Any discussion of cloud computing should begin with a clear and straightforward definition of the topic at hand. At Dopkins & Company, our preferred definition is: *Using the internet*. For those looking for a more focused translation, we offer: *Utilizing third-party resources accessible through the internet*.

A useful practice is to replace the saying "in the cloud" with the more transparent "on the internet." For example, "we have decided to put our financial information on the internet," or "we put all our confidential client information on the internet." Has a certain ring to it, right? Understanding this is a central part of any discussion of cloud computing within an organization.

The term 'cloud' itself (commonly attributed to a 1996 US Patent) was originally intended to identify a 'network,' something that was not represented by flow-charting symbols at the time.



US Patent US_5485455

The trend towards introducing third parties into the work environment, whether it is Fortune 100 companies or mom-and-pop shops, has seen a dramatic increase in the past few years.

So, what are the driving forces behind this migration to hosted services? More importantly, what are the challenges faced by organizations who choose the cloud? These topics will be covered in detail in the following pages of this whitepaper and will provide valuable takeaways for decision makers faced with the tough decision of whether to adopt a cloud solution.

A useful practice is to replace the saying "in the cloud" with the more transparent "on the internet."

Benefits of the Cloud

It may seem obvious, but the identification and selection of benefits that an organization wishes to pursue in the cloud is a crucial step in the planning process. The reason for this is that each benefit is typically accompanied by a counter-balancing risk.

Compromise is the name of the game when it comes to cloud adoption. Many companies fail to realize that approaching the cloud piecemeal may in fact be more advantageous than attempting to accomplish every goal simultaneously.

So, what are some common benefits that organizations are looking to gain in the cloud?

+ Reduce storage and archive costs
+ Allow for remote access
+ Allow for collaboration
+ Improve search efficiency
+ 24/7 access and support
+ Increased security with redundancy
+ Reduce administrative overhead

Let's take a look at three examples:

Benefit	Compromise
Reduce Storage and Archive Costs	The use of a document management solution may reduce storage and archive costs because of the provider's economies of scale, but it also requires you to **relinquish control** of your sensitive business information to a third-party provider. This loss of control, and concerns over the security and operational environment of the provider, may outweigh the cost savings.
Allow for Remote Access	Empowering employees to work from home, or other remote locations, can increase productivity but also introduces risks by **allowing data to travel** outside the four walls of the organization. Depending on the business need for remote computing, this risk may or may not overcome the improved efficiency.
24/7 Access and Support	Having access to a leveraged support team with special skills may appear to be a dream come true for many companies. Remember though, as we increase the number of individuals with **access to our data outside of the organization** we also increase security risks.

During the preliminary phases of cloud adoption make sure to vet each benefit to ensure that the organization is aware of, and willing to accept each new risk that will accompany it. The old adage remains true to this day: "slow and steady wins the race."

What is Moving to the Cloud?

The saying "as a service" has become a buzzword in the world of cloud computing, usually prefixed by an equally exciting term like security or compliance. The acronym "XaaS" has even become commonplace, referring to "Everything as a Service."

To keep things simple, let's break down the three most standard acronyms: SaaS, IaaS and PaaS. This will help you understand what companies are moving to the cloud and provide a few easy-to-remember examples for the next time you encounter the terms.

SaaS	Applications & Software
IaaS	Servers & IT Personnel
PaaS	Development Tools

Software as a Service [SaaS]

SaaS providers typically provide access to applications through the use of a web browser without the need for software to be downloaded or installed. Common examples of applications moved to the cloud are ERP systems, CRM systems and collaboration tools. If you need a hint to remember SaaS, just think of *Google Apps.* Applications like *Google Docs* are hosted remotely on *Google's* servers and can be accessed on any computer with an internet connection.

Infrastructure as a Service [IaaS]

The image of endless rows of glowing servers lining a colossal data center can serve as an illustration of infrastructure as a service. Among other services, IaaS providers commonly maintain large quantities of client data in what is known as a 'server farm.' IT Managed Services, also known as an outsourced IT department, is another popular offering from cloud service providers (CSP).

Amazon Web Services, among the first companies to pioneer IaaS, is likely the most widely known provider. *AWS* provides the back-end for many of the world's largest organizations.

Platform as a Service [PaaS]

While not as popular, the term Platform as a Service is commonly included with the previous two examples. Companies like *SalesForce.com* provide development tools, libraries and other resources for organizations looking to design a proprietary app. *SalesForce1* is the name given to their PaaS offering.

Challenges in the Cloud: Multi-layer Service Agreements

A primary concern with cloud computing is the severe lack of transparency that exists between cloud providers and their customers. Data ownership and data access issues are common.

Are you certain who owns your data when it is stored at a remote location? More specifically, do you have (in writing) the names of all entities with access to your data?

Often times, a cloud service provider will outsource certain responsibilities to another organization in order to focus on their core competencies.

The result of these relationships is that your data may be traveling between service providers unbeknownst to you. Organizations should be diligent in investigating these extensions in responsibilities.

Let us evaluate the following example: Your organization contracts with Company A to provide a cloud-based ERP system. A feature of this ERP system is its ability to process credit card payments; a service that is outsourced to (Company B) a third-party payment processing provider in NJ.

The ERP and Payment Processing vendors both use different data centers for their storage needs, located in AZ and FL.

EXAMPLE

COMPANY	COMPANY	COMPANY
[i.e. ERP System]	[i.e. Payment Processor]	[i.e. Data Center]
The company that you have contracted with directly to provide a cloud-based accounting ERP solution. You selected this system for its ability to process payment transactions.	The ERP provider outsources its payment processing function to a third-party provider, as it is not their core competency. This arrangement may not be obvious within the ERP system.	In order to provide the most efficient system performance possible, Company A outsources their data storage needs to Company C. Company B also uses a third-party data center.

“You can’t secure what you can’t see.”

“A primary concern is the lack of transparency.”

While complex multi-layer service agreements make it difficult to identify which entities are involved, as we have just discussed, it also introduces questions regarding *who* is accessing your data.

Many cloud providers will require a certain degree of privileged access to your data in order to meet your needs and provide support functions. When we increase the number of entities involved, we are likely increasing the number of these administrative users.

Edward Snowden was one such privileged administrator when he perpetrated his disclosure. What may be a surprise to you regarding the Snowden story is the relationship between Edward, his employer, and the NSA.

The NSA outsourced a significant portion of their ‘spying’ needs to consulting firm Booz Allen due to the immense amount of data they had collected. In turn, Booz Allen had to hire a number of temporary employees to handle the increased workload. Edward was one of these temporary employees, granted privileged access to the private data of millions of Americans.

This example illustrates the concern that organizations must have regarding third-party access to their sensitive data and the personnel controls employed by these vendors. This duty is still your responsibility.

EXAMPLE

The NSA is the face of the scandal. The entity that everyone knows and the sole group believed to be involved in handling the private data of the American public.

In fact, the NSA had outsourced much of their ‘spying’ activities to consulting firm Booz Allen. They performed as much, if not more, analysis of your private data than the NSA.

Edward Snowden was a temporary employee of Booz Allen Associates, not the NSA as many stories would have you believe. He executed the breach as a third-party administrator.

Challenges in the Cloud: Operational Considerations

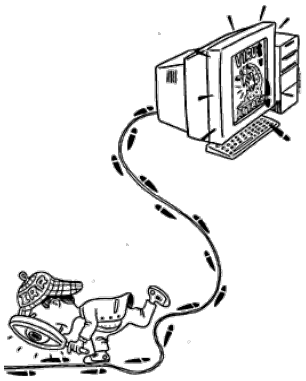
Data Backup

Reviewing your Service Level Agreement (SLA) is crucial to identifying issues between your organization's policies and procedures and those of your cloud provider. For example: data backup.

Are backups performed and destroyed on an appropriate schedule? If not, you may be exposed to unnecessary liability due to inconsistent data retention practices.

Let's say your organization's destruction policy states that emails are destroyed after 18 months, but your provider's policy is 9 months. It's easy to see the problem. Vice versa, a policy that is longer than your own can introduce legal discovery concerns.

CSPs are able to provide affordable services by being "one-size-fits-all," which may not always be the case. The benefits gained from outsourcing these responsibilities are contrasted by the risk of mis-aligned policies and practices.



Incident Response

A related issue is that of incident response. In your organization, if a problem occurs, you are able and likely to commit as many resources as needed to address the incident. In addition, you can oversee the process and become involved as needed.

This is far from the scenario faced with a third-party cloud service provider. If an incident has in fact happened, will you be notified and kept up-to-date?

Not only have you lost almost all control over the situation, but you are also in a potentially catastrophic position if the incident affects a critical piece of software or infrastructure. Being proactive and asking the right questions can help prevent these scenarios, or at least better prepare your organization.

Alternate Providers

Imagine receiving this email from your CSP: "We have filed for bankruptcy and will be terminating our services shortly. You have two weeks to download and migrate your data." Are you prepared? Have you considered an alternate provider? What if your data is maintained in a proprietary file format?

These scenarios arise frequently in the turbulent world of cloud computing. Whether it is from bankruptcy, acquisition or some other scenario, it is important to have contingencies in place for these unfortunate and unforeseen events.

When it comes to business continuity and disaster recovery, you can never be too prepared!

CSPs are able to provide affordable services by being "One-Size-Fits-All," which may not always be the case.

Threats Facing CSPs

A common misconception of small and medium-sized businesses is that they are unlikely to be impacted by a cyber attack due to their size and low profile. While there is certainly truth to this sentiment, the cloud introduces new threats to businesses of all sizes.

Cyber criminals often seek to cause as much damage or disruption as possible to a large number of businesses. For this reason cloud service providers present an enticing target. With a single attack (on the CSP, not the individual clients) a hacker can impact hundreds, if not thousands, of businesses.

More concerning is the fact that many small and medium-sized business rely on the cloud for mission critical applications and infrastructure elements. Is your organization prepared to operate without an operational ERP system, document management tool, data center or other hosted service?

Cyber Security Insurance

With so many threats facing an organization what can be done to mitigate the risks? Cyber Security Insurance is an option that is quickly gaining popularity, with 31% of companies reporting that they own a policy and 39% planning to purchase one within 12 months, according to a Ponemon Institute Research Report.[1]

While Cyber Security Insurance covers a broad range of computer and data-related threats, more focused Cloud Protection policies address the concerns of organizations operating in a hosted environment.

31% CURRENTLY HAVE CYBER INSURANCE

39% PLAN TO PURCHASE POLICY WITHIN 1 YEAR

Typically, Cloud Protection policies will cover the following topics:

- Loss of income due to vendor down time
- Costs associated with procuring new vendor
- Costs of migrating to new vendor

[1] Ponemon Institute. (2013).

Service Organization Control Reports (SOC)

Developed by the American Institute of CPAs, Service Organization Control Reports, also known as SOC and previously SAS 70 reports, have become an industry standard for cloud service providers. They provide an assessment of the internal control environment of a service provider from an independent perspective.

SOC 1 reports are intended for organizations with a direct relationship (or 'nexus') with internal control over financial reporting. SOC 2 was developed specifically for entities such as data centers and IT managed services providers, who are not directly involved in the financial reporting process. SOC 3 reports are very similar to SOC 2 reports and are commonly used more for marketing purposes than anything else. SOC 1 and 2 reports come in two types: Type 1 (Design and Implementation) and Type 2 (Operational Effectiveness).

Organizations such as *Amazon Web Services*, *SalesForce.com* and *Google Cloud Platform* provide the full spectrum of SOC reports.

SOC 1	SOC 2	SOC 3
Controls at a service organization relevant to user entities **internal control over financial reporting**.	Controls at a service organization relevant to **security**, **availability**, **processing integrity** **confidentiality**, or **privacy**.	General use report. **Coverage similar to SOC 2**.

Many companies face the question: "How can I know whether my cloud provider is secure and properly controlled?" SOC reports are a **good first step** in gaining comfort over the internal control environment of your provider.

Objectives of a standard SOC report include:

- Physical Security
- Environmental Safeguards
- Incident Management
- Change Management
- Network Access
- Data Backup
- Logical Access

Certifications

REGULATION & STANDARDS

Regulation of Protected Health Information

Payment Card Industry Data Security Standard

International Information Security Standard

US Standard Setting Body

Cloud Service Provider Security Assessment

Is your organization subject to regulation such as HIPAA or PCI? This is an extremely important question due to the significant impact it can have on your organization, both from a compliance and security perspective.

Two common misconceptions regarding regulatory compliance in a hosted environment are: liability/responsibility does not extend to cloud providers, and liability/responsibility can be transferred to a cloud provider. Let's take a brief look at both scenarios.

If your company has HIPAA regulated data (such as customer health information) that is created, received, maintained, transmitted or destroyed by a third-party, then your responsibility extends to that provider. If they breach HIPAA, you've breached HIPAA.

In a different scenario, an organization that needs to process credit cards (subject to PCI-DSS requirements) may outsource this function to a specialized cloud provider. Unfortunately, the organization is not able to pass-off their responsibility to protect those transactions and must ensure that their CSP has proper controls in place.

Many cloud service providers are getting certified to standards to illustrate their dedication to security. Remember, as an organization you are always responsible for the security of your data. Even if your provider is certified to a certain standard, it does not eliminate the need for you to also be secure.

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Information Security

Dopkins at a glance

- Founded by Leonard Dopkins in 1955
- One of the largest independently owned accounting firms in WNY
- Over 100 employees located in over 10 states
- Full service, highly technical, and diversified accounting and consulting firm

Our services

- Information Security
- Internal Audit Support
- IT Networking Consulting
- IT Network Administration
- IT Software Selection, Implementation and Training
- SOX 404 Compliance

Our certifications

Our specialists hold a variety of professional certifications, including:

- CISSP – Certified Information System Security Professional
- CISA – Certified Information Systems Auditor
- CGEIT – Certified in Governance of Enterprise IT
- CRISC – Certified in Risk & Information Systems
- Sage 300 ERP Certified Consultant
- Sage CRM Certified Consultant

Our Industries

Over 50 years of experience across a wide spectrum of businesses, industries, and situations, including:

- Healthcare/Medical
- Not-for-Profit
- Insurance Companies
- Life Sciences
- Manufacturing

Our memberships

Our team is involved with numerous professional organizations, including:

- ISACA - Information Systems Audit and Control Association
- $(ISC)^2$ – International Information Systems Security Certification Consortium
- AICPA – American Institute of Certified Public Accountants
- NYSSCPA – New York State Society of Certified Public Accountants

William M. Prohn
Managing Director

716.634.8800
wprohn@dopkins.com