eFax Corporate®

Whitepaper

Moving to the Cloud?

Pro Tips for Vetting Cloud Vendors

Moving to the Cloud?
Pro Tips for Vetting Cloud Vendors

Table of Contents

Abstract

As cloud computing becomes commonplace for many companies today, some are still working to understand which components of their core business to move to the cloud, and which applications or services to use.

Conversely, some businesses that have already moved large parts of their infrastructure to the cloud are beginning to regret their selection due to compliance and/or performance issues. Much of the time these issues are related to their cloud migration not meeting their business needs or goals.

For example, some law firms, financial institutions and manufacturing firms are landing on the hybrid model of cloud computing and finding opportunities to greatly streamline their operations with cloud-based applications like Microsoft® Office® 365, or disaster recovery and online backup services like KeepItSafe® (a j2 Cloud Services brand.)

This white paper offers practical guidance on how organizations like yours can select and implement a cloud migration smoothly, safely and cost-effectively — by avoiding the common pitfalls and knowing what questions to ask when vetting potential cloud vendors.

Executive Summary

“Survey: Businesses are Okay with Moving to the Cloud Now.”

This title of a 2016 article in the legal-industry magazine *Inside Counsel* nicely sums up a major shift in the business processes — and mindset — of an industry that is extremely careful about how it stores and transmits its data. Summarizing a 2015 survey by information-management firm Recommind, the Inside Counsel article points out that 84% of law firms are now comfortable moving operations and data to cloud services — up from 68% in recent years. Additionally, more than two-thirds of law firms say they now use cloud tools for e-billing, and more than half use the cloud for matter-management.[1]

In the report itself, called “2015 Corporate Legal Survey,” Recommind quotes a respondent explaining the industry’s increasing adoption of cloud services: “Cloud is becoming more attractive due to cost and the reality that no matter where the data is, it is accessible by someone.” Another described the migration to cloud tools as a business need: “The company does not have an in-house legal applications team, so if they want something managed, it needs to be in the cloud.”[2]

With technology continually lowering barriers to entry and increasing competition in virtually all industries, businesses are looking for ways to streamline their operations, reduce overhead, and otherwise create competitive advantages. Migrating in-house technologies and business operations to the right cloud vendors is one proven method of achieving all of these objectives.

However, by implementing their cloud migrations too hastily — without first investigating the pros and cons of moving any business-critical function to the cloud as well as the business’ overall goals and without first conducting due-diligence on any would-be cloud vendor — many businesses are finding their new cloud-based processes fraught with problems.

As the legal industry is discovering, outsourcing key processes and even an organization’s entire network infrastructure to the cloud can yield significant business benefits. But a business must first learn how to avoid the common risks in a cloud migration, as well as what to ask any potential cloud-service vendor — before making such a move.

So Many Options: How Businesses Are Leveraging Cloud Computing Today

Businesses today have tremendous flexibility in what types of services and processes they outsource to the cloud, as well as what levels of control they retain in managing those processes. Understanding the wide range of options available to you — and the pros and cons of each — will be vital to helping your team make the right cloud-migration decisions.

SaaS (Software as a Service) applications, for example, are simply third-party software tools accessible via the web. (Think Office® 365.) The applications themselves, and typically the data your organization maintains within them, are stored on the vendor's cloud. Your employees simply access the data through a web interface. These systems typically do not require maintenance or downloads from your team (although sometimes they require plug-ins to operate), but they leave little room for customization and control on the user side.

Keep in mind that SaaS providers often do not take responsibility for securing your data in the cloud. It's recommended that one check the terms and conditions as it can clearly state the cloud vendor assumes no liability for the safety of your data stored on their cloud. Moreover, a recent report from cloud-security firm Skyhigh Networks found that only 9.4% of cloud vendors encrypt customer data stored in their environment.[3]

With a **PaaS (Platform as a Service)** model, your organization maintains more control over (and responsibility for) your applications and processes. PaaS vendors — Microsoft Azure is one example — will provide you with platforms that can include an operating system, database, and programming environment. This means your team can develop customized applications for your business, while your IT team can leave much of the storage and networking management to a cloud vendor.

Finally, there is **IaaS (Infrastructure as a Service)**, the most flexible cloud computing model available. With IaaS (examples include Rackspace and HPCloud), you maintain complete control over a server in the cloud. Your team is responsible for managing the operating system, data, middleware, and applications — while your IaaS provider handles the virtualization, servers, hard drives and networking. Essentially, running an IaaS environment is like managing your own data center without having to buy or maintain any of the physical hardware.

Clearly, there is a great deal of choice today in how your organization migrates to the cloud — which applications and functions to outsource, how much customization your team wants to maintain in its processes, and what levels of control over your data you (or the regulatory bodies governing your industry) are willing to entrust to a cloud service.

Even after you have determined which of the "as a Service" options is right for your business's cloud migration, you still have to know the main mistakes to avoid in moving to the cloud, and what to look for in any cloud partner.

Common Pitfalls to Avoid in A Cloud Migration

Imagine moving much of your organization's business-critical data to a cloud storage provider — and then learning that the provider is going bankrupt.

That's what happened to more than 1,000 enterprise customers storing terabytes and even petabytes of their data with cloud storage company Nirvanix. And this lack of due-diligence is just one of several cloud-migration mistakes many businesses make.

A "Cloud Horror Story" feature in *CIO Magazine*[4] offered these common cloud-migration pitfalls:

Your cloud vendor goes out of business

When Nirvanix announced it was shutting down in 2013, it gave customers just two weeks to remove all of their data from the Nirvanix cloud — which many customers said would not be enough time, given their own bandwidth limitations. Forrester Research analyst Henry Baltazar called the timeframe "ridiculous."[5]

Your cloud vendor does not have a disaster recovery plan

Code Spaces, which let developers host code on a cloud server, was hacked in 2014. The attacker broke in to the company's Amazon Web Services account and deleted all of its users' data.

Then the cautionary tale became a genuine horror story — because the company posted a message alerting its users that it would not be able to recover the data, and that the company itself was going out of business.

As the CIO article explains, a Disaster Recovery (DR) plan is about more than simply a good backup system. A good DR plan can also include restoring data, applications, access to a server and more. That is why another cloud service gaining in popularity with enterprises is DRaaS (Disaster Recovery as Service).

Your cloud vendor's processes aren't up to acceptable standards for security and compliance

To cite just one of many horrifying examples of why 2015 has been called the Year of the Hacker, consider that data breaches against the healthcare industry alone affected the private records of more than 112 million people.[6]

As the CIO feature states, your organization's cloud infrastructure is just an extension of your own onsite data and computing services. That means you need to do thorough research into any would-be cloud vendor before entrusting your sensitive data to their services.

The Right Questions to Ask A Potential Cloud Vendor

In terms of experience, track record, and stability, cloud vendors can run the gamut — from decades-long experts serving thousands of satisfied business customers, to fly-by-night operations you should never trust with your company's data.

So how can you determine the right cloud vendors for your organization? By asking the right questions. Here are nine due-diligence questions to ask any cloud vendor that makes your short list.

1. How long have you been in business?

Because the Internet has lowered barriers to entry across so many industries, it is easier than ever for a small group to establish itself as a business — and that includes cloud vendors.

This is not to say that a new entrant into the cloud-storage field, for example, cannot be a viable vendor for your business. However, obviously the longer a company has been in business, the more experienced they are — and the more evidence you can compile of their track record with customers.

2. What is your financial position? Who is backing you?

It is unlikely that any of the 1,000+ enterprise customers storing their business-critical data with cloud provider Nirvanix had any idea that the company was headed for bankruptcy — until it was too late.

The more financially stable and well-funded a cloud vendor, the less likely your organization is to face a horror-story scenario like the one suffered by Nirvanix's customers.

3. What level of responsibility will you assume for the security and integrity of our data stored on your cloud?

Remember, cloud-security firm Skyhigh Networks found that fewer than one in 10 cloud vendors encrypt customer data as a matter of standard practice. And many cloud service Terms and Conditions clearly state that the vendor takes no responsibility to secure the user's data.

Given that a 2014 report by the Cloud Security Alliance found a typical enterprise's employees are storing company data across roughly 500 cloud applications, it is vital to your organization's security that you implement a policy of learning what level of responsibility a cloud vendor will assume before allowing your employees to place any corporate data onto that service.

4. Does your perimeter intrusion defense merely generate alerts on detecting an attempted breach, or does it proactively prevent such intrusions?

Your cloud vendor's perimeter protection system should provide it with a lightweight dynamic view of the attacks that are constantly evolving and attempting to gain access to its customers' databases and applications

This protection is not enough. That environment might already be compromised, for example, by malicious files implanted into your repositories before you put your security systems in place. Such files could remain undetected for years, waiting for the right trigger to activate them. To ensure you can detect and eliminate these risks, you also need to ask your cloud vendor about how they scan for and address such threats.

The sophisticated tools now used to locate and weed out dormant malware, tools popularly known as "defense in depth" applications, should also be a part of your cloud vendor's arsenal. Ask the vendors you are considering working with if they employ such tools in their standard processes, and if they have integrated them into their backup and recovery applications. Any vendor that has not done so should not make your short-list.

5. What levels of physical security do you employ for protecting your data centers or colocations?

To this point we've been focusing primarily on technological security measures, such as encryption, and terms and conditions, including to what level a vendor will assume responsibility for protecting your data.

But the truly trustworthy and secure providers will have a host of redundant physical security measures in place wherever they store your corporate data. What separates the trustworthy vendors here from the lesser players is that physical, onsite security requires investment, and infrastructure — and most cloud vendors simply don't have it.

You're looking here for measures such as onsite physical security guards at your vendor's data center, ideally at the facility 24/7. You also want authentication measures for access, such as badges, and even biometric readers like fingerprint or retinal scans. And you will want the facility under constant 24/7 video surveillance.

Finally, you'll want storage redundancy — ideally, with your data residing at two geographically distinct locations, with failover capability in the event that one data center experiences an outage or other disaster.

You will find that most providers simply can't afford to offer this level of physical security for your data. But the ones who can… are probably worthy of your business.

6. What security and compliance certifications have you earned?

This is a crucial question to ask any cloud vendor upfront. If your vendor for credit card processing will store your data in an offsite data center, has it passed the SSAE-16 Type-2 audit successfully — demonstrating it takes sufficient measures to address availability, security, and confidentiality of data, utilizing robust SOC control reports? Also, does your company fall under regulations mandating that its data cannot enter or leave the United States? (For instance, a law firm).

Is the vendor certified as PCI-DSS compliant, demonstrating sufficient data encryption and security processes for the payment card industry? And has the vendor been reviewed and tested against the best practices of the ISO-27002:2013 Standards, meeting the International Standards Organization's guidelines for information security management practices?

Finally, if your business is in a regulated industry — or if you handle Personally Identifiable Information (PII) or Protected Health Information (ePHI) for your clients — you will want to ask any cloud vendor on whose applications you will be storing such data whether or not their processes are compliant with the relevant regulations, such as HIPAA, GLBA or SOX.

7. What encryption protocols will you use to transmit our data?

Here you should demand nothing less than the most advanced encryption standard in use today — Transport Layer Security (TLS). Some cloud vendors will transmit your data using the outdated Secure Socket Layer (SSL), which is now considered vulnerable to attack, particularly to Man-in-the-Middle Attacks, according to the US-based SANS Institute[8], a specialist in cyber-security training.

Other vendors simply do not employ any protocols to encrypt your data for its journey across the Internet.

Entrusting your data in transit to anything less than the most sophisticated encryption in use today is not only risky, it might also land your company on the wrong side of federal regulators. Remember, data privacy regulations such as HIPAA, SOX and GLBA require "reasonable efforts" to secure and protect sensitive data in transit. Knowingly failing to encrypt such data — or encrypting it with a protocol now widely considered insufficient — can place you in non-compliance with these regulations.

8. What level of Technical Support does your cloud service include? How are your Support Engineers trained?

This is another question that will help you separate the genuine experts from the less experienced and less stable companies.

A worthy cloud service provider will be staffed 24/7 with highly trained Support professionals — available anytime by phone, email or chat. When you experience a data disaster or any type of hiccup to a function critical to your ongoing business operations, the last thing you want to hear when you contact the cloud vendor for help is a voicemail service.

9. How is activity in our cloud account monitored and recorded?

For both record-keeping and regulatory purposes, it is important that your cloud vendors track all activity in your accounts — and that they be able to provide you with a full audit trail at any time.

Better still, you should look for cloud vendors wherever possible whose platforms include an administrator portal that allows you and your team to access a comprehensive audit trail online at any time — and to generate usage reports directly from this portal.

eFax Corporate: An Easy Cloud Migration Decision

One cloud service that has proven itself for nearly two decades to significantly improve a business's processes is cloud faxing.

A cloud fax service allows your staff to send and receive faxes by email, from anywhere — desktop, laptop, smartphone, tablet, and even your company's existing multifunction printers (MFPs). An enterprise-caliber cloud fax solution allows your IT team to outsource your entire fax infrastructure to a fully hosted service operated by digital fax experts. This means you can eliminate onsite fax machines, fax servers, analog fax lines and all of the related fax architecture your IT team has to maintain today.

With the right vendor — a vendor that can answer all of the questions above to your satisfaction — migrating to a cloud fax solution can improve your company's workflow efficiency, responsiveness, cost-effectiveness and security.

If you are ready to move to a tried-and-true enterprise cloud fax solution, consider eFax Corporate® — the most widely trusted and successful cloud fax service for enterprise-level customers.

Part of the multibillion-dollar cloud services leader j2 Global® (NASDAQ: JCOM), eFax Corporate owns the patent for sending faxes by email, which is the core foundation of more efficient cloud faxing. We have developed numerous other patents over the last 20 years for sending and receiving faxes by email over IP networks better and more efficiently than workaround technologies discussed in this paper. So while Fax over IP (FoIP) and other technologies are inefficient in terms of bandwidth, frequently leading to fax errors, we leverage our patented cloud fax processes and global network to deliver your business-critical fax documents with Telecom-level completion rates compared to competitors using fax-over-IP technology stand-ins running over Voice-over-IP (VoIP) based networks.

To learn more about outsourcing to a cloud fax model with eFax Corporate, visit us at enterprise.efax.com or call Sales at (888) 532-9265.

About eFax Corporate

eFax® is the world's leading online fax solution, with more than 11 million customers worldwide. eFax lets users receive, review, edit, sign, send and store faxes by email or through a web interface. eFax offers plans for individual users and provides corporate solutions. eFax is a brand of the j2 Cloud Connect division of j2 Global®, Inc. and a registered trademark of j2 Cloud Services™, Inc. and j2 Global Holdings Ltd. Learn more at enterprise.efax.com.

Worldwide Headquarters
j2 Global, Inc.
6922 Hollywood Blvd.
Hollywood, CA 90028

Contact US Sales (888) 532-9265
email us at: corporatesales@mail.efax.com

enterprise.efax.com

Follow Us

Please Recycle