Enterprise Cloud Applications – can we trust them?[1]

Authors:

Rob Sperrey, MSc (ISG, Royal Holloway, 2015)

Geraint Price, ISG, Royal Holloway

Abstract: This article examines a number of the more significant risks involved when an enterprise utilises line of business applications hosted in the cloud. It discusses possible mitigations in order to determine which of those risks are straightforward to address and which are less easy to resolve and therefore demand special attention and understanding from management. It finds that technological aspects can often be effectively addressed but that issues of governance, compliance and remedy can remain a problem. In this way the article aims to inform and offer guidance to those responsible for commissioning or implementing a cloud-based outsourcing of their organisation's critical systems.

Introduction

A whole industry has built up around the premise that hosting line of business applications (such as Customer Resource Management, Enterprise Resource Management, Human Resource and other key applications) in the cloud can bring huge benefits in terms of cost saving and flexibility for those organisations that choose to do so. One could even question if the management of any business is really doing their job if they have not spent some time and effort seriously considering if this can work for them.

However, those with the responsibility of signing the cheques for such services, or those with the job of making sure that critical cloud based applications deliver, whilst keeping data secure and maintaining availability, can often feel a profound sense of unease and loss of control when committing a key part of their organisation to a third party cloud service provider. Therefore, it is worthwhile spending some time to consider how real the perceived risks are, if this emotional reaction is justified, and what due diligence might be appropriate in order to successfully realise the benefits.

There is a legitimate case to say that the security of cloud applications can and should be better than those of the 'islands' of in-house IT that traditionally host enterprise applications. This is because the same economies of scale that make cloud so cost compelling in general, also apply to the provision of security. A cloud provider that serves many cloud customers (or tenants) from a single infrastructure should be able to spread the cost of best of breed security over multiple tenants and thus make the provision of good security more affordable than it would be in the traditional context. So, for example, highly physically secure, redundant facilities, comprehensive controls around data

[1] This article is to be published online by Computer Weekly as part of the 2016 Royal Holloway information security thesis series. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full MSc thesis is published on the ISG's website.

handling and extensive intrusion prevention measures are now made cost effective, whereas before, an individual company could not necessarily justify such investments. Qualified and dedicated security personnel can be used to maintain and improve security assurance, when before security may, by necessity of cost, have been a non-core side-line for an individual who may also have a number of other job functions. Standards that provide a framework for security can be more cheaply, easily and coherently implemented for many tenants, instead of a reinvention of the security wheel company by company.

Of course, this assumes an ideal world, and that your cloud provider really does reinvest with a long term view that allows them to provide that improved security, and does what they say they are going to do. Therein lies the problem of cloud – the need to place trust in, and outsource responsibility to, the provider you are engaging. As we will discuss below, from the perspective of security, the technology is for the most part mature, well proven and well scrutinised. What does not necessarily match this is the transparency, continuity and in the worst case, the remedy, should a provider fail to meet their obligations.

Cloud Supply Chain

One of the characteristics of contemporary cloud offerings that reduces transparency for potential customer is the Cloud Supply Chain. This is where cloud providers themselves may outsource lower layers of their service to a third party provider. Thus, a provider offering a turnkey application (Software as a Service or SaaS) may be built on the cloud platform (in terms of servers and infrastructure) from another Platform as a Service or PaaS provider. In turn, the PaaS provider may be outsourcing infrastructure (in terms of facilities including power, heating, ventilation, and internet connectivity) to yet another (Infrastructure as a Service, or IaaS). Thus, there could be a number of interrelated suppliers involved in delivering your cloud-based line of business application. This has the potential to add complexity and risk with each additional partner in the chain, and further remove control with each layer. Your supplier may have a contract with you, which may give you some level of control over them, but you don't know what control they have over their supplier. What if the underlying supplier(s) went bust? Or was bought by a competitor of yours? Or relocated overseas to a hostile jurisdiction? Your cloud supplier may adhere to a recognised information security standard such as PCI-DSS, or ISO 27001, but how does this map to what their cloud platform supplier observes (or does not observe) in terms of standards? There are many potential pitfalls over which you will have limited visibility unless you have sufficiently high buying power to demand complete visibility.

This cloud ecosystem of multiple parties is an increasingly common practice, as suppliers specialise and focus their activities in distinct areas of an increasingly competitive market. It is surprising how many well-known cloud applications are outsourced lower down the chain (Netflix, Spotify and Foursquare all run on Amazon Web Services for example)

There are a number of models that describe various cloud models (NIST, Jericho, Cloud Security Alliance, among others) but none really pay close attention to the Cloud Supply Chain phenomenon, which deserves some serious examination when considering suppliers.

Hasn't cloud computing been around forever?

Is cloud a relatively new phenomenon, or not? Mainframe computing from the 1960s and 1970s appears, in many ways, to be very similar to certain cloud concepts. For instance, like cloud, mainframes were centralised computing infrastructure supplying computing power to large numbers of usually remotely connected users. They also have access to large quantities of data storage. They are housed in data centres, just like cloud servers. They are (or were) often owned and operated by data processing bureaus, akin to cloud service providers. Finally mainframe clustering technology (providing multiple processing platforms and failover capabilities) has been available for years. Even virtualisation (a key cloud technology) was first developed on mainframe computers.

There are, though, a number of essential characteristics that make a cloud a cloud, and they are important to consider in order to get an accurate picture of cloud and its relative security. Firstly, **on demand self-service** and the **ability to self-provision** enables cloud providers to offer flexibility with minimum human intervention and thereby lower costs. **Dynamic resource pooling** and **rapid elasticity** enable the cloud to run more efficiently and to seamlessly accommodate the peaks and troughs of customer demand; again, with no human intervention. In the mainframe context, an army of people (and associated bureaucracy and time delay) were required to achieve these things.

Looking at the technical side of cloud, it is these characteristics, controlled by the so-called Service Engine, which perhaps account for some of the major technical cloud vulnerabilities and some of the biggest headaches in providing cloud infrastructure. Attackers can and have targeted these layers to achieve Denial of Service attacks (where resources are blocked) or more specifically Economic Denial of Service (EDoS), where a cloud customer's billing record is manipulated to either increase their charges or take them above a threshold that blocks further use. The way to prevent this, and mitigate such risks, is really down to the developers of such service engines who should follow secure software development principles from the start to provide failsafe defaults and reduce the attack surface area available to the potential attacker. It is difficult for a customer to know for sure if this type of approach is taken, without having the ability to do audits on the supplier or their developers. Again, most customers are unlikely to be able to do this unless they have the buying power of a government department or FTSE100 corporation – and even then it is not guaranteed.

Proven Underlying Technology

Much of the underlying technology of the cloud is tried and tested, and as such offers high levels of security. Take **virtualisation**, a key concept within cloud.

Virtualisation is the technology that gives cloud the efficiency and economies of scale that allow cloud platform suppliers to offer computing power for fractions of a penny per unit, and that make the prospect of deploying applications in the cloud so appealing. It is a fact that the processor of a server in a traditional non-cloud scenario spends a considerable proportion of its time idle, resulting in a partially wasted asset. Virtualisation allows multiple processes, operating systems and thus tenants to run on a single processor. With multiple tenants on a processor, multiple processors on a single chip, multiple chips on a blade and multiple blades in a single server, computing density is

massively magnified, allowing costs to be amortised over many users, and the per user cost to be drastically reduced.

However, it would seem at first sight that such resource sharing by multiple tenants should bring with it compromises in security. In fact, virtualisation has been around for many years – firstly in mainframe computers, then later on developed as part of grid computing, before arriving in servers as we know them today. As such, software implementations of virtualisation have iterated a number of times, incorporating lessons learned and paying attention to important security principles and have reached a level generally accepted as secure. Furthermore processor vendors including Intel and AMD have developed their products to match this, incorporating additional levels of hardware-based protection which makes compromising a virtual machine much harder.

Scrutiny and peer-review have driven this improvement in security. Despite previously identified theoretical attacks, vulnerabilities are few and far between, as can be evidenced by a search of the relevant public sources such as the NIST National Vulnerability Database.

"Blue Pill"

One of the more famous exploits aimed at undermining virtualisation technology, called "Blue Pill", was devised by Joanna Rutkowska, a Polish cyber security researcher. The name of this exploit was inspired by the film The Matrix (where the protagonists accessed a world within a world by taking a blue pill). The exploit involved the silent introduction of a malicious virtual environment underneath a legitimate one, and thereby compromising it and giving control to the malicious environment. The critical view of this was that, while this is a theoretical possibility, it is relatively easy to detect with the right precautions. This scrutiny by multiple parties is an example of how information security evolves and improves.

Another technological aspect of cloud that is sometimes supposed to be a weak spot in its security, concerns data transfer. Intercepting data in transit (either between the cloud and the users, or within the various elements of the cloud) could be a primary method of attacking a cloud-based application. However, in reality , proven technological solutions have been applied to address this. Data in transit within and between clouds can be protected with IPSec (which is mandated as part of IPv6), and data communicated between the cloud and individual users can be protected with SSL in the same way we routinely protect online banking or shopping transactions. These technologies are successfully used to protect the data of millions of users every day. We cannot regard them as inviolable, but depending on the criticality and value of the data concerned, they are generally regarded as good enough. Furthermore, virtual switches and firewalls, and intrusion detection and prevention devices can, if deployed properly, be used to harden these environments even further. Penetration testing (agreed with the cloud service provider) can be used to prove the efficacy of these measures and give a level of assurance for the potential customer.

Data Protection

Another potential cloud headache concerns privacy and the legislation that protects us all against misuse of our personal data. The UK Data Protection Act, and its international equivalents, mandates that reasonable precautions should be taken to protect data against unauthorised disclosure. This includes that it should not be held offshore unless in a jurisdiction with recognised reciprocal legislation and accountability. In fact, anonymisation, tokenisation, or encryption of data are

methods that can provide adequate protection for these purposes (see the UK Information Commissioner's anonymisation code of practice) There is undoubtedly a cost to implementing these measures, but they are powerful tools that can address a significant risk.

Encryption also offers a simple, immediate, and manageable way to overcome another potential cloud concern of data deletion (if you try to delete your data, is it really deleted or does it persist on some other part of the cloud provider's infrastructure, for example other parts of a disk array or backups). If data held in the cloud is encrypted, its effective deletion becomes as simple as destroying the key with which it is encrypted. Of course, if this route is chosen, careful key management then becomes vital – though there are a number of ways to do this.

Contract

Some of the issues discussed above, and their remedies, hopefully illustrate that many of the security issues in the cloud are addressed with robust technological controls. However, this does takes time, effort and cost to implement. Cost that comes out of the bottom line profit of the cloud service provider. There is always the worry that providers may not do what they say they do, and things can always go wrong.

However, if the worst happens, that's what you've got a contract for, right? Unfortunately, not necessarily. Ongoing research carried out by the Queen Mary University of London Cloud Legal Project (CLP) reveals that the majority of cloud contracts involve fixed conditions that cannot be individually negotiated between the provider and the customer and often with unfavourable terms for the customer. As we have touched on above, only a very big fish can hope to negotiate their own contracts and thus appropriate safeguards.

Another key point highlighted by the CLP study is that the majority of the contracts have a limitation of liability built into them that restricts the amount a supplier may be due to pay as compensation. This is usually limited to the value of the services they have provided to you.

This amount can differ significantly when compared to the expense incurred from downtime, loss of sensitive data, or reputational damage. This significant exposure really takes the teeth out of any legal safeguards the cloud customer may believe they have. The different tiers in the cloud supply chain described above can act as a risk multiplier and it is easy to see how the customer can be left exposed.

These factors underline how important it is that the customers take steps to do their own due diligence around their provider.

Standards

Standards can play an important part in cloud computing, and it is possible to find suppliers that operate their businesses in accordance with relevant standards such as PCI-DSS, ISO 9001 and others. They may self-certify against these standards or they may have commissioned third party audits, but it is unlikely they will allow individual customers to perform full audits for reasons of cost, and confidentiality for other customers. It is important to try to make sure that any applicable standard is relevant and comprehensively observed, and is not just on a cloud provider's boilerplate for marketing reasons.

Conclusions

Cloud computing offers services which, given the right precautions, can be as secure, if not more secure, than a traditional non-outsourced context. However, this comes at a cost and it is important for anyone involved in a potential move to cloud-based applications to retain some of the resulting savings for management and contingency planning.

When selecting a supplier, the more information they supply about their security standards and practices the better. In this way it is possible to build up some idea of how seriously they take security. It is reassuring to see that some of the larger and more established cloud providers use security as a market differentiator to attract potential customers to their service. As such they provide transparency around their security architectures and management, allow scrutiny by third party auditors and even offer the possibility for customers (or their contractors) to perform penetration testing against their systems, allowing them to see for themselves if relevant risks have been addressed. This follows a key principle of information security which holds that peer-review delivers a much greater level of assurance than 'security by obscurity'.

The risks discussed above are not by any means an exhaustive list of potential security concerns around cloud computing. Anyone wishing to make themselves fully aware of the risks, their relative seriousness and their potential mitigations can access the full version of the dissertation from which this article was drawn. Comprehensive studies in this area have also been carried out by organisations such as ENISA (European Network and information Security Agency), and the CSA (Cloud Security Alliance) who maintain resources for guidance in this area.

Biography:

Rob Sperrey MSc is an alumnus of the Royal Holloway ISG Information Security Masters programme and a Certified Information Systems Security Professional (CISSP). Prior to this he spent most of the previous twenty years based in the Netherlands developing new markets in Europe for a series of North American technology vendors active in the Unified Messaging and secure IP networking sectors. He also spent a period of time involved with the definition of a global managed services proposition for Vodafone's fixed-mobile convergence service. Rob is a consultant with Stratia Consulting, an organisation providing information assurance services to government, defence and industry.

Dr Geraint Price BSc (London), PhD (Cantab) obtained his B.Sc. in Computer Science from Royal Holloway University of London in 1994 and his Ph.D. from University of Cambridge in 1999. His Ph.D. dissertation analysed the interaction between Computer Security and Fault Tolerance. From 1999 to 2001, he was a Research Associate within the University of Cambridge, working on projects related to Denial of Service attacks in networks. In November 2001, he joined the Information Security Group (ISG) as a Research Assistant to work on a project funded by PricewaterhouseCoopers on the future of Public Key Infrastructures. From late 2002 to mid 2004 he worked on a research project funded by the PKI Club at Royal Holloway. In Sept 2004 Geraint was appointed as Lecturer in Information Security. Geraint has a strong interest in the practice of information security and leads the ISG's external engagement activities with business and government. Geraint is a regular attendee, panellist and speaker at a number of industrial fora, including I-4 and the ISF.