



**An ISSA UK and Secoda Risk
Management White Paper**

THE SECURITY IMPLICATIONS OF CLOUD COMPUTING

*Author: Adrian Wright
Director of Projects ISSA-UK
Managing Director
Secoda Risk Management Ltd*

15 February 2010

Contents

Introduction	2
About this paper	2
Confidentiality & attribution	2
Session objectives	3
Workshop dates & venues	3
Delegate feedback	3
Workshop topics	3
Event benefits	3
Workshop tasks	4
Session: cloud computing	5
Benefits of cloud computing	6
Risks of cloud computing	7
Summary of key conclusions	10
Speaker biographies	13
Company information	13
Reference materials	14
Acknowledgements	14

Introduction

Two of the most important risk topics to emerge in the last year are the explosive emergence of cloud computing and the growing risks presented by insiders within organisations.

Both of these trends are fuelled by the need to cut staffing and technology costs, but organisations need to be vigilant in measuring and controlling risk in order to remain safe.

Member interest in these topics prompted the ISSA in conjunction with Secoda Risk Management to organise a series of three, half day workshop seminars for regional ISSA groups, which were kindly hosted by our sponsors KPMG. These highly interactive workshops brought together practitioners of information security, audit and risk from all sectors including finance, health, education and local government; each bringing their own unique perspectives and experiences on the risks and benefits of using cloud-based services and how they are assessing and addressing their respective insider threats.

About this paper

This paper brings together and summarises the various risks, benefits and practical tips arising from all three workshop events for the benefit of attendees and the ISSA membership as a whole. This white paper covers the security implications of the **Cloud Computing** stream from the above workshop sessions. A companion white paper is also available which deals with the **Managing Insider Threats** topic.

Confidentiality & attribution

Workshop sessions were conducted under the Chatham House Rule¹ thereby allowing attendees to speak freely about their experiences, concerns and security measures without compromising their organisation's privacy.

Consequently, apart from the presenters, no attendee organisation or individual is associated with the various issues or controls noted in this paper, or any other material arising from these sessions but only noted by industry sector where appropriate.

¹ <http://www.chathamhouse.org.uk/about/chathamhouserule/>

Session objectives

The presentations and workshop sessions enabled attendees to identify the benefits and risks associated with Cloud Computing and via moderated workshop sessions, to discover the techniques their peers were using to balance risk and reward in today's challenging economy.

Handouts provided before and during these sessions, copies of the PowerPoint presentations used during the sessions and at a subsequent summary presentation given at the ISSA Chapter Meeting on 10th December along with the findings in this paper and its companion white paper on Managing Insider Threats, comprise the 'takeaway' deliverables being made available to workshop attendees and the ISSA membership overall.

Workshop dates and venues

Three half day presentations + workshops

- Edinburgh 20th Nov 09
- Bristol 27th Nov 09
- Manchester 4th Dec 09

Delegate feedback

Overall, attendees rated all workshops at 5/5 – 100% satisfaction. Below are selections of comments from the feedback forms:

'Well focused'

'Workshops useful and interesting for exchanging ideas'

'Firstly many thanks for putting on a great event at Bristol on Friday. It was excellent to network with other IT professionals and the structure of the day (i.e. the workshop programme) allowed us to share ideas and concepts. It also continued to generate much conversation on the walk back to the train station!'

'Can I say what a very enjoyable time Friday was. I felt that the event was exceptionally productive and insightful. I look forward to seeing the results of the Whitepaper.'

'It was a most enjoyable session and really got me back into thinking the "correct" way'.

'I enjoyed the format and makes a change from the normal PowerPoint presentations'

'Refreshing to be able to interact with peers within a meeting'

Workshop topics

1: Examine the security implications of Cloud Computing and define a checklist of the key issues and necessary controls

Each workshop was preceded by a short presentation to introduce the topic, give examples and state the format and desired outcomes for the workshop itself. Delegates were divided into two teams of between 6-12 people per team working in different areas and then brought back to the main room to present their respective conclusions to the whole audience.

Event Benefits

- Sharing of knowledge, experience and solutions cross-sector
- Brainstorming to uncover unforeseen issues & controls
- Encourage information sharing on these topics
- Networking opportunities and connections
- Produce useful guidance & checklists
- Platform for further work in these areas

Workshop Tasks

Each team was tasked with the following actions to discuss, prioritise and then present back to the main group. Moderators oversaw each session and collated the collective output of all workshops; the summarised results of which form the basis of this report.

- Consider the various types of and uses for Cloud Computing, and derive a common set of 'use cases' that can be used to assess the risk / reward balance;
- Identify the types of risks involved, and whether these are new or changed risks or levels of risk compared to traditional service delivery models;
- Define at a high level a list of technical, procedural, legal, framework (e.g. policies) and contractual controls to maximise benefits and mitigate any risks;
- Produce a checklist of controls that could form the basis of a detailed audit plan;
- Nominate a spokesperson to present your list to the main audience, and;
- Be prepared to answer questions or justify particular inclusions or omissions.

Workshop Session: Security in Cloud Computing

The Cloud is here to stay

According to IDC, worldwide forecast for cloud services in 2009 will be in the order of \$17.4bn. The estimation for 2013 amounts to \$44.2bn (+50% pa), with the European market ranging from €971m in 2008 to €6,005m in 2013.

Even if your organisation has no immediate plans to deploy or move to cloud-based services - the chances are you may already be using cloud or SaaS without realising it. The phenomenal growth of social and business networking sites is just one example group.

Today's cloud-based backup, storage and processing facilities can be acquired and setup within an hour by non-technical staff and paid for on a personal credit card. However, it is vital to understand where your valuable data is, what the legal considerations are, and how to get your data back if you need to. This workshop session explored these questions and enabled participants to create a checklist of issues and corresponding controls to manage risk.

Types of Cloud Computing

Cloud computing can refer to several different service types, including Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The latter is sometimes referred to as 'utility computing'. There are differing security implications within each of these categories, and these need to be examined accordingly. Furthermore, there are different classes of 'cloud', which may also be divided into:

Public: available publicly - any organisation may subscribe. Example: Google Apps.

Private: services built according to cloud computing principles, but accessible only within a private network

Partner: cloud services offered by a provider to a limited and well-defined number of parties.

Again the security characteristics of each of these classes of service will be different – along with the levels of reliability, trust and costs associated with each one.

Definitions

One of the most confusing issues surrounding the cloud and its related services is the lack of agreed-upon definitions. As with all emerging technologies, the lack of clarity and agreement often hinders the overall evaluation and adoption of that technology. Two groups that have offered a baseline of definitions are the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance. NIST's definition of what Cloud Computing is:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

The full text can be found at: <http://csrc.nist.gov/groups/SNS/cloud-computing/>

Benefits of Cloud Computing

Staffing and Skills

Significant savings can be made compared to traditional in-house hosting and delivery of services, as many or all of the necessary technical, administrative and support staff and skills required to setup, deliver and support the services are provided by the cloud provider within the cost of the service.

Hardware, Software and Infrastructure

Removing or reducing the need to buy, install, maintain and support internal systems hardware, software and licenses, energy, cooling, and provision of secure manned premises represent some of the largest areas of cost saving associated with moving applications to the cloud.

Replaces Capital Expenditure with Operational

For many organisations it is more difficult to justify and obtain capital expenditure (Capex) than operational expenditure (Opex). This may be because the SaaS type model is typically low cost and much easier to slot into an OPEX budget stream, and you are less committed to keep paying than if you invest in equipment outright.

Pay only for what you use

The whole point about cloud computing, and particularly infrastructure-as-a-service, is that you don't utilise 100% of your IT 24x7. If you did, you would probably be better off buying all your own hardware from a purely economic standpoint. But cloud providers allow you to deploy new servers in minutes and pay based on hourly usage, which has a huge impact on the economics. So, even with an average utilisation as high as 70% (and that's quite high!), you would likely be better off using Amazon EC2 than buying your own hardware.

Some of the biggest savings to be made and at the lowest risk to business are in the area of systems development and test platforms. Many large organisations currently invest millions on building development and test networks that mirror as closely as possible their production IT environment. This allows them to functionally test, load test, and perform change management operations within a near-real network, yet maintain total segregation from production systems.

Clearly this is a very costly arrangement to maintain over the longer term, particularly as the utilisation levels of such testbed systems is usually very low. Doubling-up R&D systems as part of your BCP/DR strategy helps justify some of the cost of these systems, but rarely all.

On the other hand, cloud networks like EC2 and Microsoft Azure are ideally suited to providing massive amounts of computing and storage which can be setup in minutes, pay per CPU cycle or storage MB, and then tear down (and stop paying) as soon as you've finished. Examples abound of how people have set up the equivalent of a whole data centre of compute power, applications and storage in minutes to test a particular application or crack a computational problem, and done it all for a couple of hundred dollars. The cloud is highly suited to this type of task, and the cost benefits are massive compared to owning and running the infrastructure yourself.

Agility

The cloud promises to deliver attributes such as increased agility, elasticity, storage capacity and redundancy to manage information assets. The true value of cloud environments is in helping manage the entire application lifecycle e.g. *Development > Test & QA > Deployment > Production > Change & Upgrade > Support* and so on. Increased agility, i.e. the ability to get up and running with new products and services faster, combined with the ability to scale up or down on-demand to handle unexpected loads and so prevent loss of business due to decreased performance or outright downtime, are some of the primary benefits to be had in the cloud.

Green Credentials

Shared infrastructure is inherently more environmentally sustainable than dedicated infrastructure. Utilisation level per server, network or data centre will be kept very high in a cloud vendor service because it needs to be so in order to show a profit, while keeping the cost to the user low compared to owning their own resource. This means that less hardware, power, cooling and other resources are consumed on a per-user or per customer basis, than if every user or customer organisation ran all their own systems and data centres.

Risks of Cloud Computing

The following is a high level summary of the technical and non-technical risks associated with moving data into the cloud. Cloud applications are inherently more vulnerable to external threats than those managed inside well-protected organisations; though data in the cloud can be protected by implementing robust security mechanisms and by developers building security into their products at the design stage. Furthermore, through careful selection of which platforms, applications and information one chooses to migrate to the cloud, it is possible to strike the right balance between risk and reward.

Loss of Information Governance

Transference of information and operations to a third party inherently also transfers a number of governance issues to them, upon which you have to trust they will carry out to yours, your customer's and perhaps your regulator's satisfaction. SLAs and compliance to common security policies has some value, but you are essentially blind to what is actually going on. For example, the provider's infrastructure must be secure; which often precludes your ability to conduct penetration testing such as may be required under PCI-DSS. Unclear ownership responsibilities for assets, high staff turnover rates in outsourced locations and incorrect handling of personal sensitive data, are some of the issues that may arise in moving to cloud-based services.

Compliance Risks

Some types of businesses need to pay special attention to the data security issues that arise when migrating to the cloud: Businesses that operate under strict regulatory conditions like Sarbanes-Oxley, SEC or FSA regulated businesses, or specialist sensitive areas like pharmaceuticals and defence.

Storage or processing of sensitive types of data in multiple locations and outside of jurisdictions bound by EU data protection laws could give rise to non-compliance issues for users of public cloud services. This also means that in some cases using a public cloud infrastructure implies that certain compliance requirements cannot be achieved. For example, Amazon EC2 says customers would be "hard pressed" to achieve PCI compliance on their platform, implying that EC2 hosted services may not be used to handle credit card transactions if full compliance with PCI-DSS is also needed.

Isolation Failure

By definition, cloud services are multi-tenancy. That is to say that different customers share common system, storage and network resources, and customers are only segregated from one another as well as the operating systems, virtualisation and network management will allow. A security vulnerability or flaw in the virtualisation 'hypervisor'², misoperation of network management systems, or malicious activity of customer seeking to gain access to other user's information could result in information being exposed to non-authorised entities, corrupted or lost.

² <http://en.wikipedia.org/wiki/Hypervisor>

Malware presents a particular risk. Organisations tend to be well protected internally due to the use of secure gateways and anti-malware checking at the perimeter and all end points, both within the boundary and on mobile platforms. By contrast, many of the endpoints in a cloud setup are outside of your control and may be under the control of numerous other parties. Similarly, the concept of a securely controlled perimeter between the Internet and your proprietary applications and data may be difficult to maintain and prove. Furthermore, given the large quantities of data that can be obtained from a single breach, we must assume that this opportunity has not been missed by potential attackers and that cloud providers will become an increasingly lucrative target for malicious intruders.

Legal and Political Risks

Cloud infrastructure, support and intervening networks may traverse global networks, with data residing or being processed in a variety of locations (*see section on Compliance risks and Salesforce.com example in Summary Conclusions*).

The process of Legal Discovery is often used to force companies to find and hand over information in litigation cases, and companies in the US have faced severe financial penalties for failing to produce data when requested. Here in the UK, there are similar obligations to find all data and information when required by a DPA subject access request or under the Freedom of Information Act in the public sector. Doing this quickly when you don't know where all your data is physically located, where all backup copies of the data are, and what the legal implications are of recovering data held in one country for use in a legal case being held in another are, could all prove problematic.

Apart from the vagaries of different laws in different jurisdictions and any regulatory compliance risks, it should be remembered that many governments assume the right to see or intercept all information held and processed within their borders; the highest profile example being the US Patriot Act. Also uncertainties may arise if data centres are located in high-risk countries, e.g. those lacking the rule of law or having an unpredictable legal framework and enforcement, autocratic police states or states that do not respect international agreements etc. Sites could be raided by local authorities and data or systems subject to enforced disclosure or seizure.

Many countries do not have equivalents of the Computer Misuse Act or effective data protection or intellectual property legislation in place. Safeguarding valuable information that passes through, or is processed or held in such regions could be difficult to achieve and even harder to obtain redress if things go wrong.

Capacity Overrun

As discussed above in context of the benefits of pay-per-use and environmental sustainability; cloud services are run at high levels of utilisation in order to deliver maximum cost benefits in a 'greener' way. The flip side of this benefit is the risk that overall capacity, or your virtualised portion of it, may not be able to cope with spikes in demand.

For example, one popular use of public cloud infrastructure will be to facilitate remote working by staff. If pandemic or other widespread events like the floods we saw several years ago caused a large proportion of workers to have to work from home; it is possible or even likely that shared infrastructure and networks, e.g. the internet itself, might not have sufficient spare capacity to meet demand, and services might fail as a result.

There is an emerging school of thought that current pandemic plans of most organisations will fail if invoked, due to the 50:1 contention ratio of most domestic ADSL broadband connections. If a large proportion of the working population was forced to work from home during a pandemic, severe weather or some other crisis that precluded staff travelling to the office - there is a real risk that 'last mile' contention for bandwidth would prevent most people from working online. Similar capacity bottlenecks could, and do exist elsewhere in any systems infrastructure that relies on the use of publicly contended-for resources.

Data not encrypted end-to-end

In these days of massive data losses or leakage and the extensive measures organisations are putting in place to prevent it; the cloud will present both opportunities and threats to data loss prevention (DLP).

Most DLP measures work by ensuring that sensitive data remains encrypted when it is outside of the organisation, or when removed from a protected organisational asset – e.g. a worker's encrypted laptop, onto a memory stick, or CD. However in the case of software-as-a-service (SaaS), it is not possible to keep information encrypted throughout, because information must be unencrypted in order to be processed or used. Consequently if any processing is required in the cloud, we cannot be certain that no-one outside of our business will see it, so it could become lost, stolen or modified at some point in the cloud, by anyone able to gain access to vendor processing facilities, support functions or networks.

Service outages backup and recovery

Cloud providers should obviously guarantee your data is safe and recovered in the event of a failure or disaster. However it is often unclear to what extent and frequency data is backed up, and whether full recovery can or will be made in the event of a major or widespread incident.

BCP and DR plans are only really proven when a data loss incident occurs, and many backup processes fail to recover all data. When you own, manage and test these processes it is possible to establish a reasonably high level of confidence that they will work; but reliance on cloud providers to do the same on your behalf is largely an act of faith.

Google Apps and Amazon AWS and EC2 have recently had major outages where customers were unable to access their applications and data for up to 22 hours. In the case of the latter, a major outage resulted in permanent loss of customer data with no hope of recovering it.

A recent history of Cloud Provider Service Outages:

Salesforce.com outage

<http://www.datacenterknowledge.com/archives/2010/01/04/salesforce-com-hit-by-one-hour-outage/>

Rackspace Outage

http://www.thaindian.com/newsportal/tech-news/rackspace-outage-affects-several-sites_100291843.html

Blackberry Outage

http://www.pcworld.com/article/185397/blackberry_outage_rim_should_compensate_users.html

Twitter Outage

<http://www.themoneytimes.com/featured/20091218/twitter-restored-after-being-hacked-id-1094523.html>

Amazon Outage

http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_qci1376474,00.html

Microsoft Sidekick Outage

<http://tech.blorge.com/Structure:%20/2009/10/11/microsofts-sidekick-cloud-outage-gets-worse/>

Reliance on public networks

The internet is inherently insecure, unmanaged and vulnerable to attack from anyone within it. As outlined above in *Capacity Overrun*, it may not cope well with surges in demand, or connected systems can fall prey to DDoS attacks, botnets or other web threats. Google Apps and Amazon AWS and EC2 have previously had major outages where customers were unable to access their applications and data for up to 22 hours (*see examples above*)

Critical infrastructure

Anyone who has worked in IT for more than 15 years will have seen how one or two vendors emerge as leaders over all the others whereupon their particular operating system, router, browser, or database becomes the de facto industry standard.

This helps drive standardisation through user popularity and means we don't all have to get trained on dozens of different platforms and applications. There is no reason to suppose that this will not also happen in the cloud provider market; much as Google has established supreme dominance in the search engine space with nearly 70% of all searches globally.

If one specific cloud services provider was to emerge as the de facto provider of cloud services, to the same extent that Google has in its space; would that provider become an attractive target for say, cyber-terrorism?

One thing is certain; as more corporate data moves into the cloud, the cloud providers will become an increasingly lucrative target for cyber crime.

Summary of Key Conclusions

Don't pilot cloud using critical applications and processes.

- While cloud computing is not in itself new technology – merely a new way of delivering computing resources; it is still uncharted territory for most organisations and certainly in the case of mission-critical applications. However, like its precursor outsourcing, the senior management of most organisations will likely again be lured by the promise of cost and manpower reduction and consequently put pressure on IT to migrate the most cost-consuming business applications (often the most critical ones) to the cloud as soon as possible. So the general consensus was to try to resist proposals to migrate mission critical applications to the cloud until the full risk implications, operability issues and costs are better understood.
- A more favoured approach, and one better suited to current vendor offerings, is to pilot the use of cloud using a number of smaller, non mission-critical applications to test the water and gain experience before committing higher value applications to the cloud.
- Key to all of this is to establish a set of clear policies and approval procedures that spell out the organisation's strategy on cloud computing / SaaS and the processes by which approval must be sought to move in-house applications and data into the cloud. Without such policies in place, there is a real danger of staff and managers simply taking the law into their own hands and setting up cloud applications without regard to the risk and business implications of doing so.

Need to shortcut audit selection – e.g. SAS 70

- The need to build a right-to-audit as a mandatory or discretionary process into cloud provider agreements is an obvious must-have. However, cloud infrastructure is and will continue to be a difficult and therefore costly, environment to audit fully using traditional methods. This is due to a number of factors such as multi-tenancy (i.e. *which parts of the vendor's infrastructure and networks is my data being processed, stored or conveyed by?*), the fact that a vendor's cloud offering is probably not all under that specific vendor's control or ownership (e.g. the Internet, payment processing, secured remote backup etc), and the fact that your data may be broken up and processed or distributed via diverse paths, be traversing networks and systems in different jurisdictions under disparate laws whereby you may have no rights to investigate – even if you knew where and what these were. This potential inability to fully, quickly and cost-effectively audit the whole structure could leave unidentified risks or incur costs that outweigh any promised benefits of moving to cloud computing.
- One possible future solution might consist of cloud service vendors themselves (or an initial customer for a service) commissioning an independent SAS70³ or similar

³ <http://www.tech-faq.com/sas-70.shtml>

comprehensive audit review, the results of which, e.g. in the form of a SAS 70 Type II certification for the service, could be made visible to subsequent prospective users as a means of building up trust. This would significantly shortcut the time, cost and resources that would otherwise be needed if every new customer carried out their own full reviews prior to taking on a service. At present there is little evidence that this is happening across all cloud service providers, but it is expected to become more of a customer requirement in future, as the true costs of cloud adoption become clear.

Fallback & back-out are as important as implementation

- One of the key risks identified was that of 'vendor lock-in'. In other words, having migrated your internal business applications and data to a particular vendor's cloud service and performed all of the required customisations and setup to make it work; how difficult will it be to back-out of the arrangement or move to another service if you need to later?
- Contained within this set of risks is the question of whether you will be able to get your data back quickly if you need to. With so many new cloud vendors and services appearing on the market, it is certain that not all will survive and many will end up being acquired by other providers – along with all your valuable data and processes.
- Traditional ways of offsetting vendor or supply risks such as software escrow or second sourcing won't work in these scenarios, so there will always be a significant area of residual risk around what happens if a vendor goes bust, gets acquired, or decides to change its terms, business model, or infrastructure to something incompatible with your operation.
- All of this gives rise to a requirement for a kind of 'reverse project planning' where the commercial, legal, technical, cost and downtime implications all need to be examined and planned within the scope of the initial project to migrate a business application to the cloud. In other words you need a clear back-out and recovery plan in place as part of any plan to move in-house processes and operations to the cloud.

Understand & prove data paths & storage locations

- Compliance is an important consideration for nearly all organisations; particularly in regard to the processing of sensitive personal data, company records, and payment card data. One example that was used during all the workshop sessions was that of Salesforce.com – a long established provider of cloud-based CRM services. Salesforce.com has traditionally relied on its two data centres in the US to process and store data on behalf of its customers globally. Clearly this situation already raises questions for UK customers who need to remain compliant with UK Data Protection, and these issues may or may not already be dealt with under the US 'Safe Harbor' scheme, which specifically provides for comparable controls over personal data originating from DPA-bound jurisdictions such as the EU. However, they are presently building a third data centre in Singapore which will not only service Asia Pacific customers, but also provide 'follow-the-sun' operational coverage in support of customers globally. Again, the legal, compliance and political implications for UK based users and their clients is not yet widely understood and therefore could be considered a risk until these issues are clarified by each prospective adopter of these or similar services.
- Understanding where your data will be stored and processed, what networks it will traverse and what legal and political jurisdictions it will cross on the way; are all questions you may need answers to in order to demonstrate compliance with EU and international law, and to address any customer, staff, or ICO questions concerning the whereabouts and security of personal information.

Vulnerable to external events e.g. pandemic

- Moving a previously in-house delivered operation to the cloud by its very nature exposes that service and its information to risks which may be difficult to foresee and which in any case are completely outside of your control. For example, service outsourcing – which cloud fundamentally is – typically reduces costs by moving anything requiring manpower, to poorer parts of the world where staffing and other costs are much lower. Usual examples being China, India, Philippines and Malaysia. Unfortunately some of these same geographic locations suffer from much higher risks of flooding, earthquakes, tornados and disease than say, here in the UK.
- Other risks such as political uprisings, local regulation, terrorism (e.g. Mumbai attacks in November 2008), and strikes, may affect service availability or operation. For example; in India during 2007, 389 industrial disputes were reported involving 0.72 million workers and resulting in loss of 27.17 million man-days. Of these, the private sector accounted for 321 (82.52%) of disputes and the public sector 68 (17.48%) of disputes reported. Additionally India has as many as 20 public holidays each year plus many religious and regional ones. Consequently, even if your organisation has not consciously embarked on outsourcing to such regions, the adoption of cloud services which are operated within or from offshore facilities could expose services to availability and support issues regardless.

Summary point:

The costs associated with preventing, de-risking, or dealing with the consequences of the above issues could easily outweigh any anticipated cost benefits. Therefore full assessment of these costs and potential impacts should be carried out as part of any decision-making process to utilise cloud-based services.

A positive security example:

There are certain types of business applications where the use of cloud computing may actually be preferable from a security risk standpoint than using traditional models of service delivery.

For example: Consider a hypothetical information service to provide news or similar low-to-medium value information to external users via the web. Using the 'old' paradigm of securing external access to internal systems and data; the standard way of providing such a service might be to allow all of the external users access to the organisation's systems and data.

However, by using cloud-based platforms and applications, it is now possible to provide faster and more accessible services while keeping any untrusted users outside of your security and ownership boundary. So assuming our data is non-critical from a privacy or regulatory standpoint, and we have been able to satisfy ourselves that the service provider has reasonable security controls in place; from a security risk manager's perspective, the cloud-based scenario may appear more attractive compared to the prospect of allowing many external users to have inbound access to internal systems and resources.

Speaker Biographies

Your Presenters and Moderators

Adrian Wright is one of the UK's most experienced technology risk practitioners. With 25 years in IT, 8 years as global head of information security at Reuters and more recently founder and lead consultant at Secoda Risk Management, he lectures and consults globally on all aspects of information security, governance risk and compliance. His key clients include FTSE 100 listed companies and other blue chip names in all sectors plus SME's and professional bodies. Adrian is a Certified Information Systems Auditor and Director of Projects for ISSA-UK.

Contact details: adrian.wright@secoda.com tel: +44 (0)8456 4 27001 / +44 (0)780 363 9704

Website: www.secoda.com

Nick Thomas is a knowledgeable security professional with over a decade of experience supporting organisations and their information security needs. Nick is an active board member of the ISSA UK Chapter and product specialist at Qualys where his role helps businesses address their security and compliance requirements. Nick is an advocate of cloud computing and passionately offers solutions involving the 'as a service' model.

Contact details: nthomas@qualys.com tel: +44 (0)1753 872094 / + 44 (0)7701 036 696

Website: www.qualys.com

About Secoda and the ISSA

Secoda Risk Management: Was formed in 2002 by former heads of Information Security and Technology Risk Management from some of the world's best-known organisations. Secoda develops, sells and maintains the RuleSafe suite of GRC software applications, as well as providing the support and consulting services on which many thousands of corporate users depend for their employee GRC programmes.

Our mission is one of continual evolution and development of high quality products and services that uniquely serve our customer's GRC needs, through our software, professional solutions, services and consulting operations. www.secoda.com

ISSA: The Information Systems Security Association (ISSA) is a not-for-profit, international organisation of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial and government.

ISSA was formed over 25 years ago and now has over 10,000 members in over 140 chapters worldwide, of which ISSA-UK is the second largest ISSA chapter in the world with a membership base of over 1500 and growing at a rate of 12%.

With active participation from individuals and chapters all over the world, the ISSA is the largest international, not-for-profit association specifically for information security professionals. www.issa-uk.org

Reference Materials

Several good reference sources on Cloud Security were put forward.

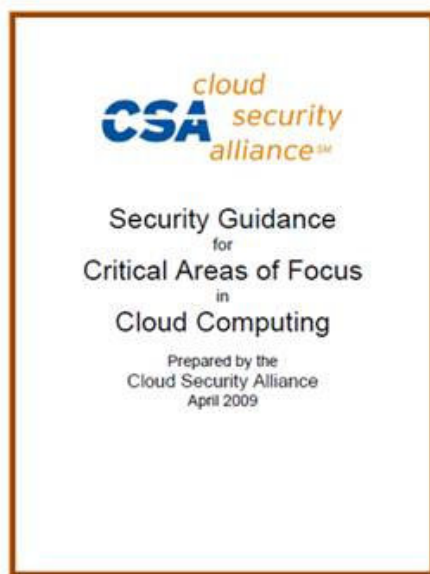
The Cloud Security Alliance has issued a document which is now in second revision, identifying the points to consider and assess when evaluating a move to the cloud.

European Network and Information Security Agency (ENISA) have similarly released some public documents on Cloud Security; (1) The Cloud Computing Information Assurance Framework, and (2) Cloud Computing: Benefits, Risks and Recommendations for Information Security.

Copies in PDF format may be downloaded free from these organisations' sites.

CloudSecurityAlliance.org

www.enisa.europa.eu



Acknowledgements

We wish to acknowledge and express thanks to the following individuals and sponsor organisations for kindly agreeing to contribute their time and resources to help host and deliver these workshops:

- KPMG – sponsors and workshop venue hosts
- Nick Thomas – VP Internet Services ISSA-UK; speaker and workshop co-moderator
- Geoff Harris – President of ISSA-UK; workshop organisation and management
- Roger Ellis – Treasurer of ISSA-UK; workshop co-moderator
- Sophie Wingrove – Administrator ISSA-UK; workshop organisation and facilitation
- Louis Gamon – Director of Administration and Alliances ISSA-UK; workshop co-moderator

end. Doc version 1.3 Release date 15 Feb 2010