



Cloud Computing

Securing your use of “the cloud”

Piers Wilson

Managing Principal Consultant, Adviza Consultants Ltd

www.adviza.co.uk





Introduction – Who am I?

- Piers Wilson
 - RHUL MSc Information Security, 1996
 - CESG CLAS Consultant
 - CISMP
 - MBCS CITP
- Managing Principal Consultant at **Adviza Consultants**
 - Formerly Head of Technical Assurance at Siemens Insight Consulting
- Contact:
 - piers.wilson@adviza.co.uk
 - 07850 905941
 - www.adviza.co.uk

Adviza Overview



- Adviza are an **independent** provider of services and solutions for **Risk Management, Information Security and Business Continuity**.
- Influential in developing and shaping the industry:
 - ITIL Service Continuity;
 - OGC Management of Risk Guide;
 - BS 25999 Part 1 & 2 (and formerly PAS 56);
 - BS 25777;
 - BS 31100.
- Involvement and understanding across industries and geographical sectors.
- Provide a set of **professional, cost effective and tailored services and solutions** to individual client requirements.

Agenda



- The cloud – a new way of working
- New security problems
- New security solutions





The cloud – a new way of working

Or is it?



Is “cloud computing” new at all?

- Yes and No
 - It borrows concepts from IT outsourcing and hosting
 - It is akin to SAAS (software as a service)
 - It is a descendant of ASP (application service provision)
- For every cloud application you could argue that if payment handling, storage and processing are “applications” then many cloud services are SaaS/ASP with a new name
 - “Cloud” has a greater hype index than SAAS or ASP though



There are some differences though

- The ownership and level of control
 - IT outsourcing tended to mean “your environment”
 - Even if things like helpdesks and data centres were shared
 - The combination of virtualisation means that if you rent a server (as with hosting) in the cloud, if its virtual, then no actual physical server may exist
 - So the cloud vs. hosting difference is almost whether you can “touch” the thing
 - There is a greater level of abstraction at the application level
 - So Google web/cloud-based applications aren’t an outsourced environment or a hosted server, they are just application functions
- So take (for example) salesforce.com
 - ASP, Software-as-a-service or Cloud ?



Easiest definition...

Whatever the end result or service...

- “Cloud” simply means that the service* is delivered via a web interface over the Internet (usually)
 - The Governments proposed G-Cloud might run over the governments own network or parts might be hosted by larger departments

i.e. :

- Different from direct network links, managed servers etc.
- Different from web based software you install on your own network
- Different from client applications you install on workstations

Can be publicly/privately/group accessible

*service in this context can mean anything



New security problems

Or are they?

How do we keep control of all this...



- Leaving aside the claims from various product vendors and service providers there are some inherent differences in how security is achieved and monitored
- Chiefly:
 - Data location
 - Third party reliance
 - Access control
 - Liabilities
 - Forensics



What control do we need ...

- Validate and assess suppliers carefully
 - If they go bust, what happens to:
 - the services your business needs?
 - More importantly, your data?
 - Can it be extracted? How? How quickly? In a format you can use?
- What information will they be handling
 - and what **confidentiality** and **integrity** requirements do you have?
 - Who will now have access to it?
- Compliance
 - Cross border data flows, international storage, jurisdiction of contracts etc. are all challenges that business might not have faced before...
 - What legal liabilities and comeback do you have?



Information risks

- Are you storing trade secrets, proprietary IP
 - Do the cloud company have access?
 - Do your competitors use the same service?
 - Do you carry out audits? Do your competitors?
 - What might they see?
 - What controls are actually in place and how effective?
- Operationally...
 - You will need to change your security policies, business continuity arrangements, incident handling and forensic policies etc...
 - Forensics especially tricky (in terms of collecting information and in such a way that it could be used for prosecution)
 - You might be able to turn off your own dedicated system – but how would this work in a cloud?
- Draw up plans to get access to information – how does this work? And how quickly?



New solutions

Or updated 'older' solutions...

Transparency



- Having robust security controls is one thing...
 - Proving it is another
 - How much transparency though?
 - Not enough leads to uncertainty
 - Too much might open the door to information leakage



- So how much do you (and hence any other customers) want to see?
 - What records do you expect to be kept?
 - How accessible is your information (i.e. who)?
 - How is segregation enforced?
- What **preventative**, **detective** and **reactive** controls are there?

Privacy

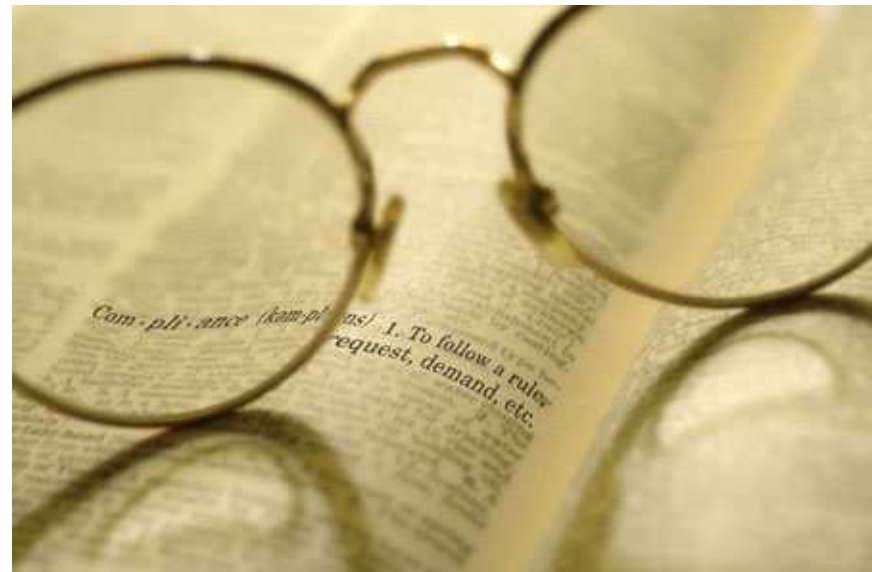


- Data privacy and protection of personal data now a truly global concern
 - Data protection legislation varies and introduces requirements around security, reporting and information access and accuracy
- These communication channels must be established
 - E.g. Subject Access Request
 - Who deals with these at your organisation?
 - Can they get access to the data they will need to respond?
 - If not who do they contact?
 - Can they get the information and how fast?
 - Is the data query you need available in the application?
- Aside from the security and data transfer requirements
- What if your data privacy requirements change after you've committed to a service

Compliance



- Variety of laws and regulations
 - May have to provide information on demand
 - Extracting it in isolation not always easy
- Trans-border information flow
 - Physical location can be an issue
 - (you might not know its happening)
- Jurisdiction
 - Of contracts
 - What is allowed in one place might be illegal in another and required somewhere else
- **Most important** – define your requirements !



Certification



- Decide what certifications you will trust and ask for them
 - ISO27001
 - BS25999
 - SAS70
 - Etc.
- Validate the scope of certifications
- External audits/penetration tests
 - Do you trust these?
 - What is assessed?
 - Check the risk assessments match your profile
- How much value would you place in a local/country specific certification?

Is there a silver lining?

- Cloud computing is an evolution of past IT/service delivery models
- There are business benefits, but these might be outweighed by real compliance and security problems
 - There may be some things that your company shouldn't put in the cloud
 - It doesn't mean there aren't other things that they could
- Like most things in security, the risks can often be managed if they are **understood** and **thought** about



Risk & Information
Assurance Specialists



Risk & Information
Assurance Specialists



Thank you for your attention...

Contact us at:

piers.wilson@adviza.co.uk

www.adviza.co.uk

Mobile: +44 (0) 7850 905941

91-93 High Street
Camberley
Surrey
GU15 3RN

Switchboard: +44(0)1276 482970

Fax: +44(0)1276 482979