



# Cloud Computing

## How secure and resilient are clouds anyway?

Piers Wilson

Managing Principal Consultant, Adviza Consultants Ltd

[www.adviza.co.uk](http://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**
- Contact:
  - [piers.wilson@adviza.co.uk](mailto:piers.wilson@adviza.co.uk)
  - 07850 905941
  - [www.adviza.co.uk](http://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 standards and industry
- 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
- And some interesting resilience challenges





## 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, hosting, 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 Government’s 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

\*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
  - What assurances and controls do they offer – and what comeback do you have if controls fail
- What information will they be handling
  - 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 obligations do you have?

# Information risks



- Are you storing trade secrets, proprietary IP
  - Do the cloud company staff 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

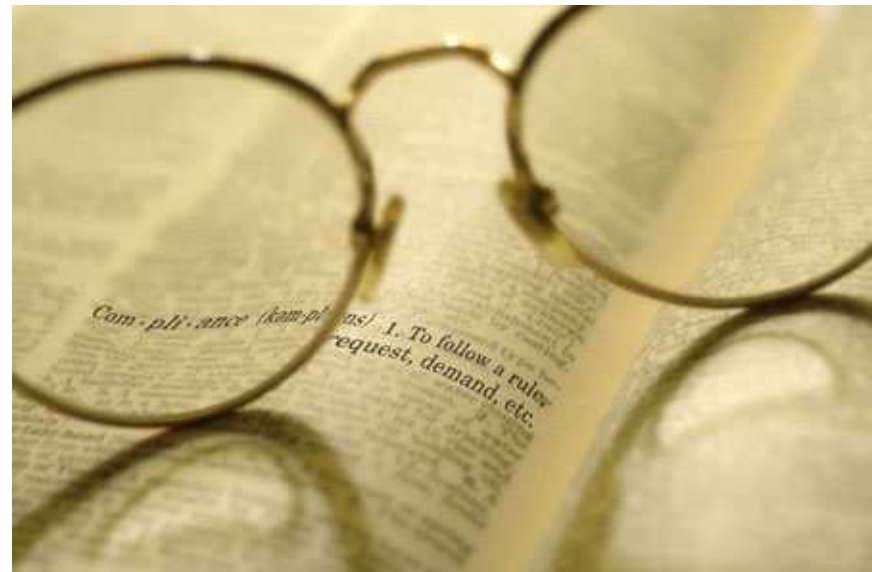


- Data privacy and protection of personal data now a truly global concern
  - Data protection legislation varies and introduces requirements around security, reporting and information access and accuracy
- These communication channels must be established
  - E.g. Subject Access Request
    - Who deals 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?



## A question of resilience

A different look at continuity



## Clouds increase resilience (?)

---

- One of the major sales messages for cloud computing is that it can provide greater resilience
  - Secure, virtualised, resilient, global, replicated data centres
    - Did I mention resilient
- **But !!!!!**
  - **What** if you need to terminate a service or change providers
  - **What** if a service you rely on ceases to operate
  - **What** if the secure, resilient cloud provider goes bust
- Think about your data/systems...
  - Can it be extracted? How? How quickly? In a format you can use? Have you got space to put it on?

# Getting clear of the clouds

- **Virtualised servers**

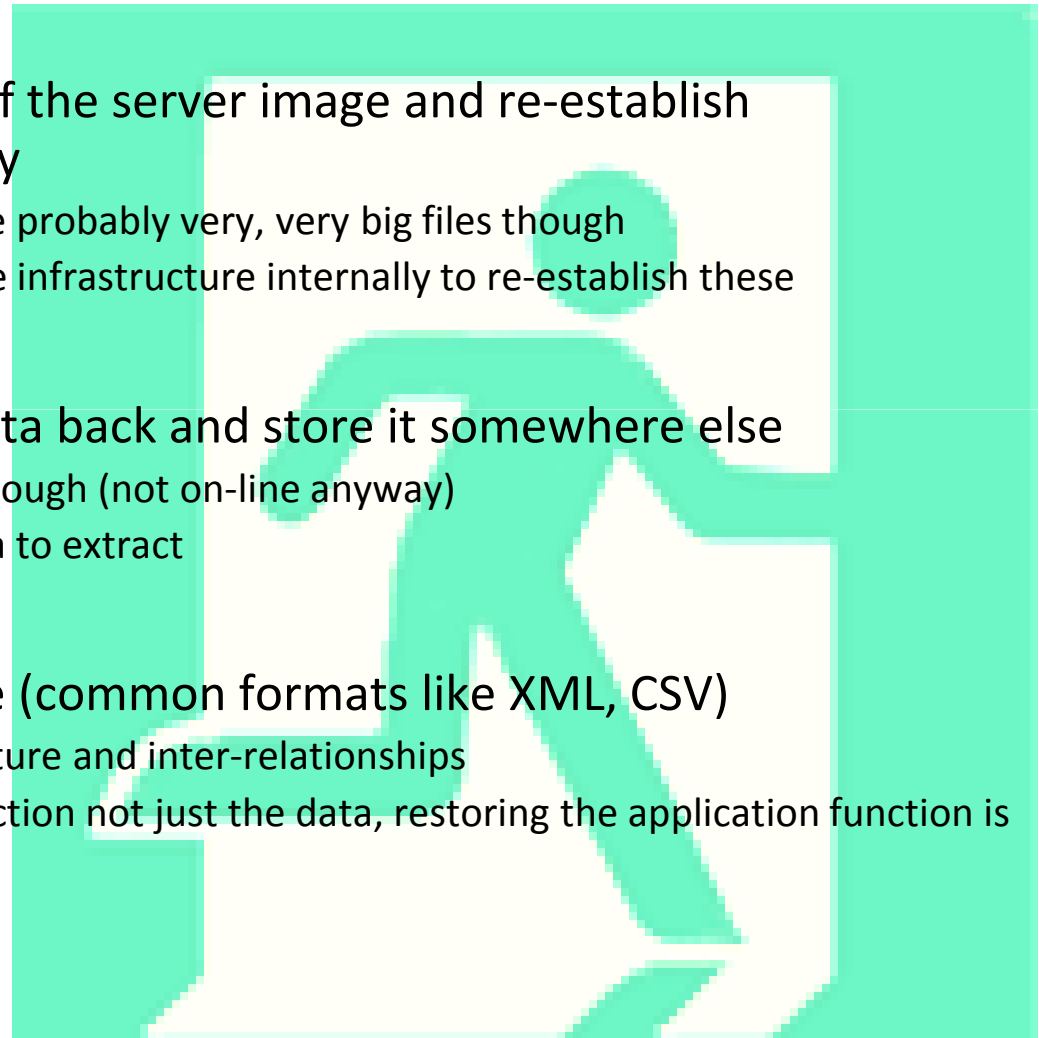
- **Probably** could get hold of the server image and re-establish somewhere else/internally
  - Note that server images are probably very, very big files though
  - You might not have suitable infrastructure internally to re-establish these

- **Data storage/archiving**

- **Probably** could get the data back and store it somewhere else
  - Most likely not internally though (not on-line anyway)
  - There might be a lot of data to extract

- **Software as a service**

- Data **might** be extractable (common formats like XML, CSV)
  - Probably will lose the structure and inter-relationships
  - Your business used the function not just the data, restoring the application function is not obvious





## My (paranoid) hypothesis...

---

- Getting “out of a cloud” might be difficult...

**I hypothesise that a situation could occur where there was a “run” on a cloud (provider)**

- This would be similar to a run on a bank
  - The effects would be similar...

# What would “a run on a cloud” look like?



- **First** it would need confidence in a cloud business to be dented in the same way a bank’s trustworthiness might
  - Perhaps the cloud company has over-extended itself in IT infrastructure and was having trouble paying creditors
  - Maybe its service levels were hit by some freak event and it had difficulty covering the penalties
  - Maybe it lost a big contract it was banking on
  - Maybe there was some knock on effect from a crisis of faith in the cloud computing industry caused by problems elsewhere
    - i.e. Could a “systemic failure” occur as in the financial sector
- **Any conceivable scenario could occur**



## Dominoes start to fall

---

- Once bad news hits the press/market there is a risk that people start (collectively) thinking  
*“Quick – we must act! Our cloud provider might go bankrupt!”*
- At this point my “run” prediction may start coming true...  
perhaps something like the following...

# The “Run on the Cloud”

1. Customers who have got the ability to extract/dump their data (virtual machines, stored files) start contacting the cloud provider to request data extracts
  - *Manually or Electronically*
2. Customers start trying to download databases, virtual machines, documents or stored data over the Internet
3. Normal response times for operations or data extractions take longer
4. Network bandwidth slows right down
5. These further problems cause further market/customer concern
6. Everybody starts to think there really is something wrong and starts extracting data/VMs/files
7. Data extraction requests/downloads increase



# The run continues



8. The provider starts spending **most** or **all** of its effort on network bandwidth management and manual data extractions

## Then, as the crisis deepens:

9. The cloud provider runs out of network capacity
  - or even media, and can't extract any more data/VMs/files for customers
10. No further requests to get access to data can be handled
  - At this point customers can't access their data, use the service or get out of the cloud
  - The available network bandwidth is choked by multiple large scale downloads
  - Downloads which frequently timeout and have to be restarted
11. Customers phone up to complain etc
12. The cloud provider staff are powerless
13. Customers by this point are unlikely to be wanting to pay any bills – cash flow suffers, penalty clauses and service credits kick in
  - the banks and other creditors/suppliers of the cloud provider notice this
14. The banks move in, the network connection is cut and the provider has to admit defeat ... **Where does this leave the customers**

# Reality or hyperbole

---



## This might sound fanciful

- But if your cloud provider hit trouble, wouldn't you (and probably several other customers) try to get out of the arrangement...
  - ... This could easily make the problems worse
- No one predicted:
  - Several high profile bank runs/failures Lehman Brothers, Northern Rock, Merrill Lynch etc.
  - Previously also people had faith in Barings, Enron, a.n.other major corporate collapse...

# Fall out (of the clouds)



- So **resilience** can fail
  - Data can be unavailable
    - If it is available it might not be usable or accessible
  - If your provider fails (for any reason) you might have to wait to get it back
    - If you get it at all
  - You might lose control over what happens to it
    - E.g. When a provider goes into administration
- The “run” scenario simply recognises that the failure (or suspicion of impending failure) could build its own momentum and make things worse

## 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, resilience 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





---

**Thank you for your attention...**

Contact us at:

[piers.wilson@adviza.co.uk](mailto:piers.wilson@adviza.co.uk)  
[www.adviza.co.uk](http://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