Edge Hill University

Cloud Computing

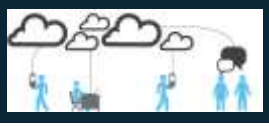
Topic 8A, Session 6

Contents

- What will make clouds attractive
- What won't make clouds attractive
- Infrastructure Security
- Identity and Access Management
- Privacy
- Audit and Compliance
- The Future of Cloud Security
- Summary

Introduction

- *Cloud computing is a powerful idea*
- *There is potential for cloud computing*
- *No Binary answers for Cloud adoption -There is a need to consider the future impact (whether to adopt or not)*



What will make clouds attractive ?

- *Low cost*
- *Flexibility*
- *Correlation between cost and usage*
- *Business functions can acquire services they need (without IT Services Dept.)*

What will make clouds attractive ?

- Low levels of initial investment and ongoing costs, economies of scale, open standards, and sustainability.
- ***Scalability on demand/flexibility to the business***
  - Reduced hardware infrastructure costs
  - Reduced IT staffing/administration costs
- ***Access to skills capabilities we have no interest in developing in-house***

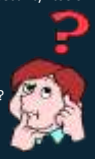
What won't make clouds attractive

- Loss of control
- Perceived risk
- Data security, financial cost
- Integration issues/difficulties
- ***Security concerns***
  - Integration with existing systems
  - Loss of control over data
  - Availability concerns
  - Performance issues
- ***IT governance issues***
  - Regulatory/compliance concerns
  - Dissatisfaction with vendor offerings/pricing
  - Ability to bring systems back in-house
  - Lack of customization opportunities
  - Measuring Return On Investment (ROI)

Infrastructure Security

- At network, application and host level, problems are exacerbated by clouds, but not caused by them
- There is a need for secure software development life cycles
- Majority of concern is over the shift in trust boundaries between users and CSPs
- Lack of Transparency – Typically limited visibility of data from security tools. Compliance, where available, is only as reliable as its scope.
- Most people are not sure what that move is

How do you know?



Identity and Access Management (IAM)

- IAM is a major hurdle for enterprise solutions using cloud
- Leads to risks in
  - Protecting sensitive information
  - Sustaining compliance
- Solutions exist, but scaling up to cloud volumes (users and resources) is an issue
- Also a need for federation and integration with directory services

Privacy

- Significant challenges due to cross country boundaries (e.g. Legal, regulatory, compliance)
- How to deal with cross-border data flows. Since this involves a number of foreign jurisdictions, complexities start to develop due to conflicting rules among foreign governments.
- Easier to define with CSP which country hosts the data, but harder to say which server
- The organisation that collected the data holds responsibility

- Information governance must be put in place that:
  - Provides tools and procedures for classifying information and assessing risk.
  - Establishes policies for cloud-based processing based upon risk and value of asset.

Audit and Compliance

- CSP needs to choose a compliance framework to suit its customers (but will all customers be covered under one!)
- Policies supported by processes and controls are a must
- Development of IT Governance, Risk and Compliance (GRC) programme is growing

The Future of Cloud Security

- Greater level of agreement (and transparency) concerning the capabilities of CSP and customer. Particularly in relation to SPI delivery model
- Developments in cryptographic research
- The development of identity-aware cloud services which map access policies across boundaries
- Cloud APIs that cover not only development and deployment, but also access management
- Cloud management services being developed by third party suppliers
- Standardised interactions/interoperations between cloud environments
- Augmentation of laws to support international operation
- Cross-CSP compliance frameworks

Summary

- Cloud computing is not a change in technology
  - The techs involved already existed
- It is, however, a change in business model
  - The biggest change is the multitenancy aspect of the model
- There is a need for greater transparency (and auditing) of CSPs to boost customer confidence
  - Most of this lack of confidence is based on unfamiliarity – the "newness" of cloud
  - Also provides opportunity for third party suppliers to develop tools to assist


Thank
You
The End