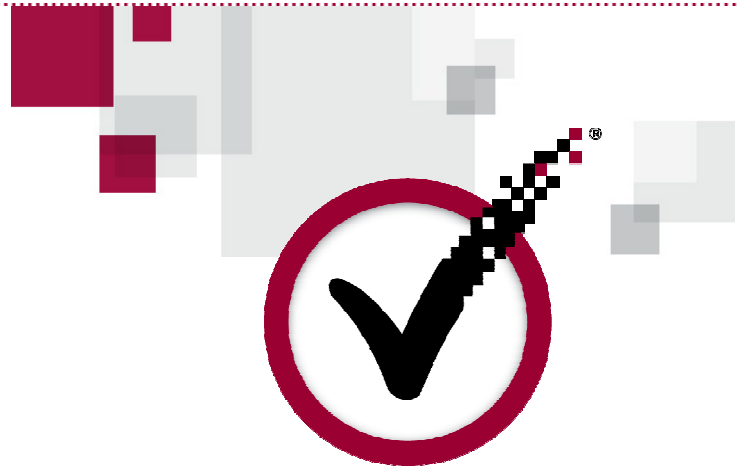
VeriSign

iDEFENSE



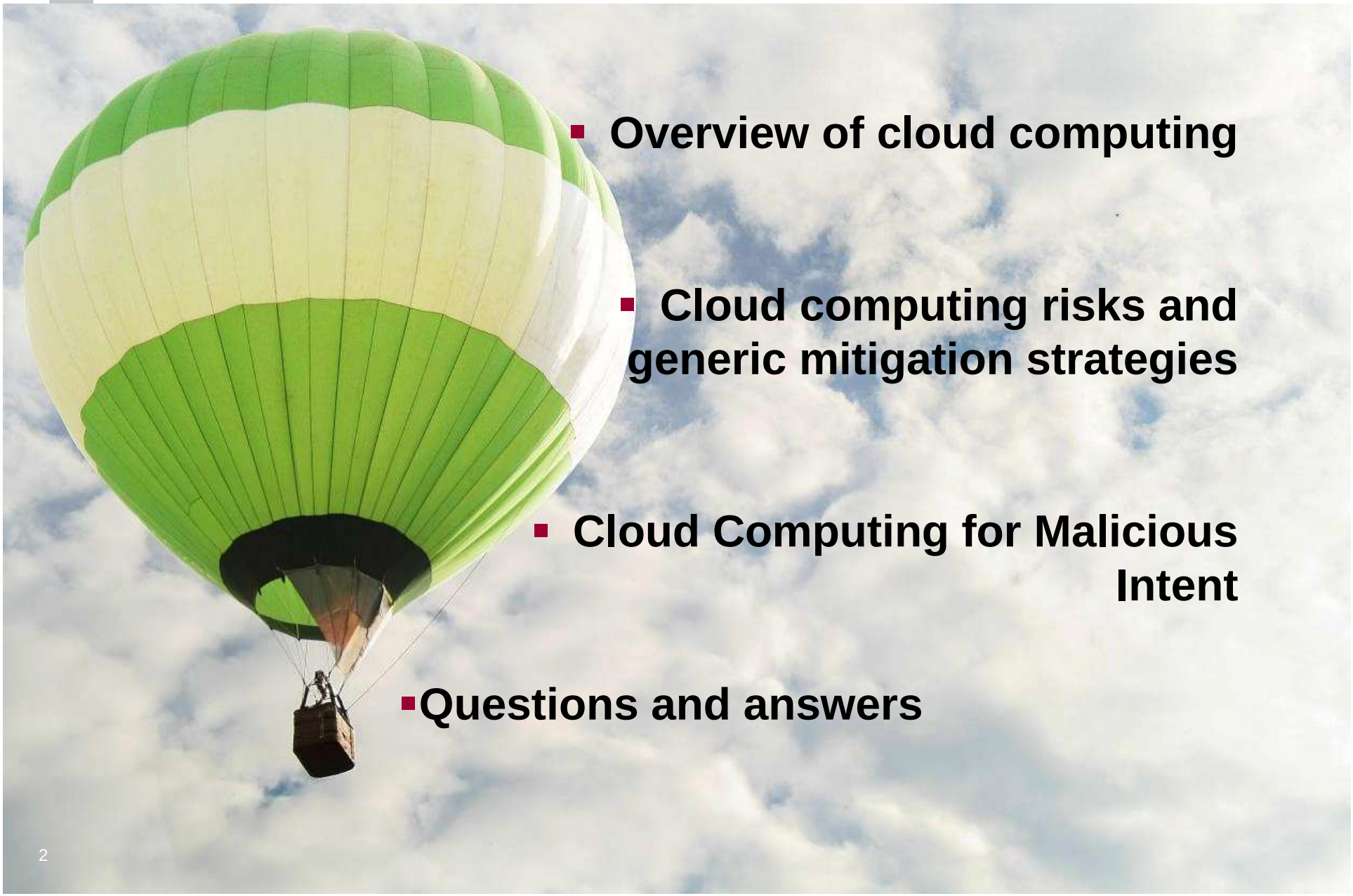
Cloud Computing

Enterprise Risks and Mitigation

Anchises M. G. de Paula
iDefense Intelligence Analyst
adepaula@verisign.com
December 4, 2009

GTS - 14

Agenda



- Overview of cloud computing
- Cloud computing risks and generic mitigation strategies
- Cloud Computing for Malicious Intent
- Questions and answers

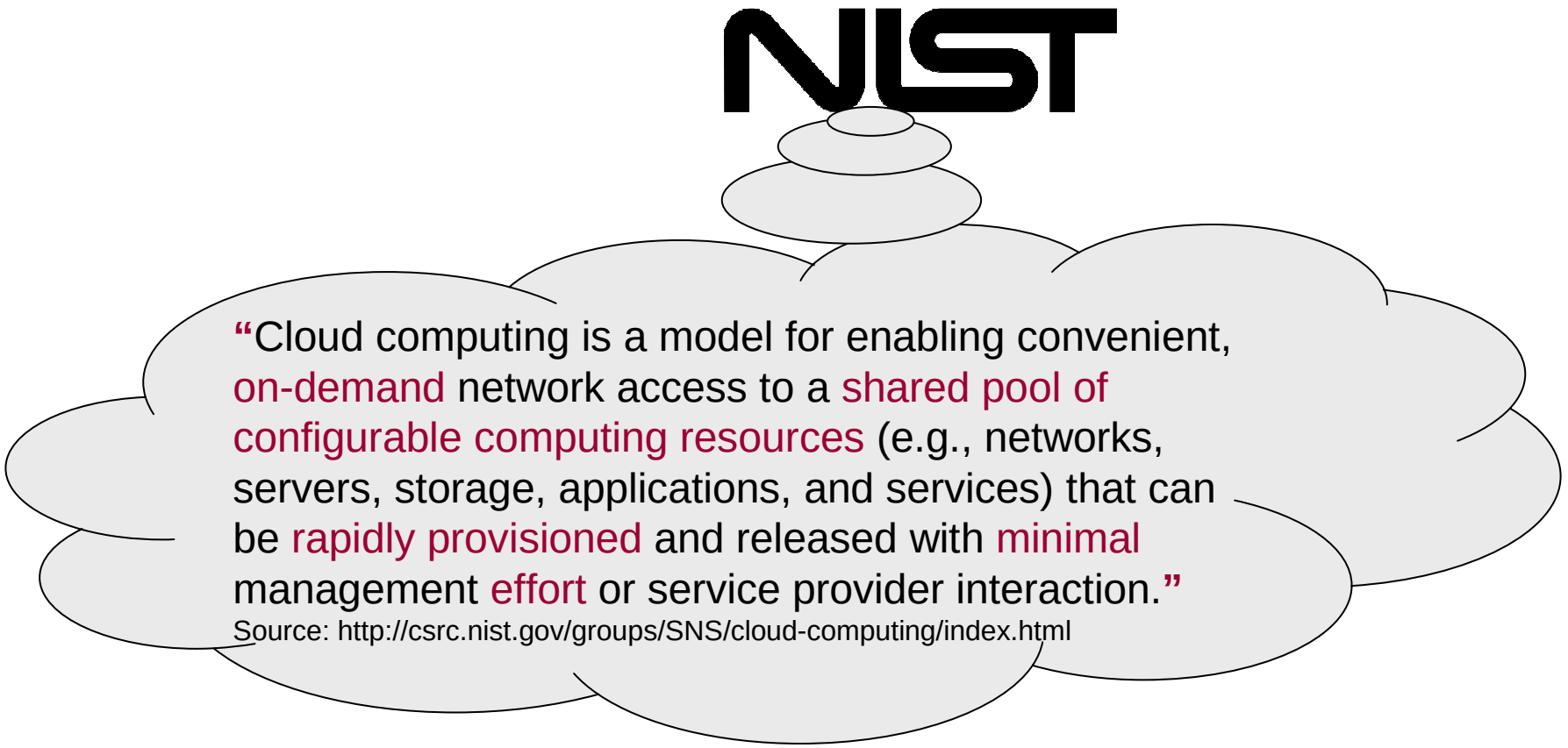
Overview of cloud computing

Overview

- The term “cloud computing” is poorly defined

Overview

- The term “cloud computing” is poorly defined



Overview

- The term “cloud computing” is poorly defined

Overview

- The term “cloud computing” is poorly defined

Overview

- The term “cloud computing” is poorly defined

- Multiple vendors, multiple definitions

Overview

- The term “cloud computing” is poorly defined

cloud security alliance

NIST

- Multiple vendors, multiple definitions
- Utility pricing model

Overview

- The term “cloud computing” is poorly defined

cloud security alliance

NIST

- Multiple vendors, multiple definitions
- Utility pricing model

- Cloud-based Service Provider (CSP) handle burden of resources

Overview

- Three basic categories for cloud computing technologies:
  - Infrastructure as a Service (IaaS)

Overview

- Three basic categories for cloud computing technologies:
  - Infrastructure as a Service (IaaS)

  - Platform as a Service (PaaS)

Overview

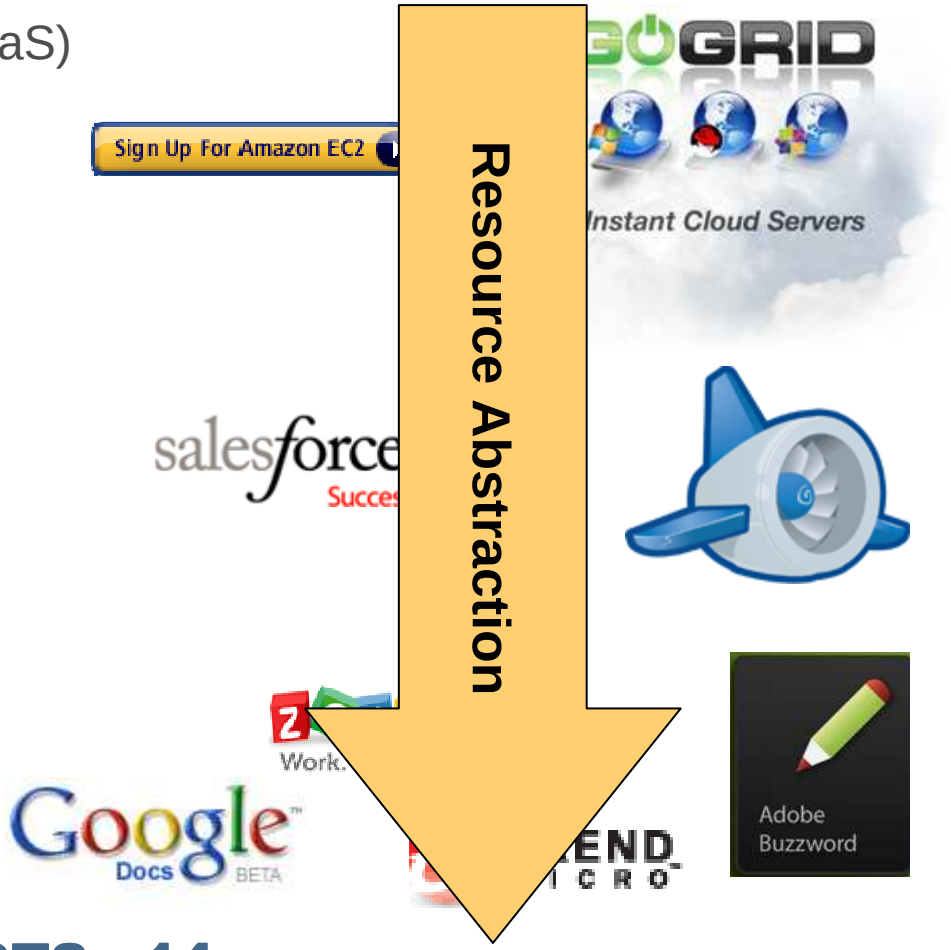
- Three basic categories for cloud computing technologies:
  - Infrastructure as a Service (IaaS)

  - Platform as a Service (PaaS)

  - Software as a Service (SaaS)

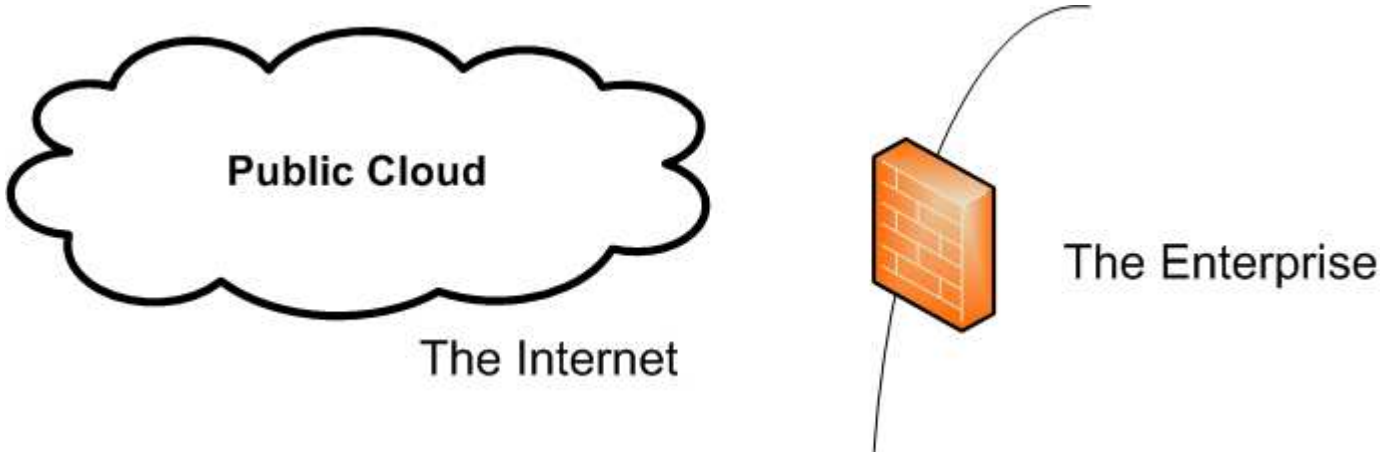
Overview

- Three basic categories for cloud computing technologies:
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)



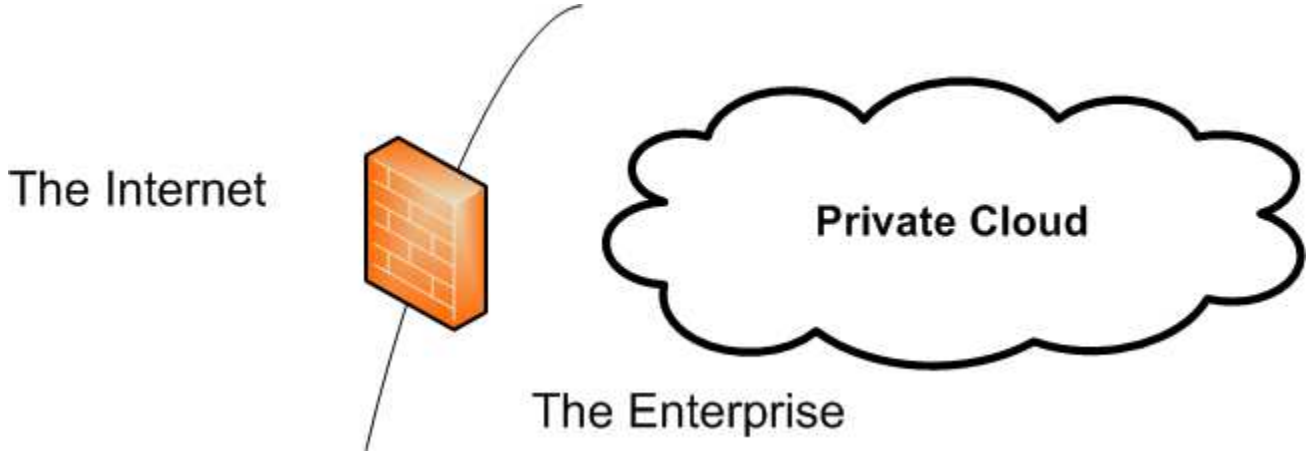
Variations on a Theme

- Public Cloud



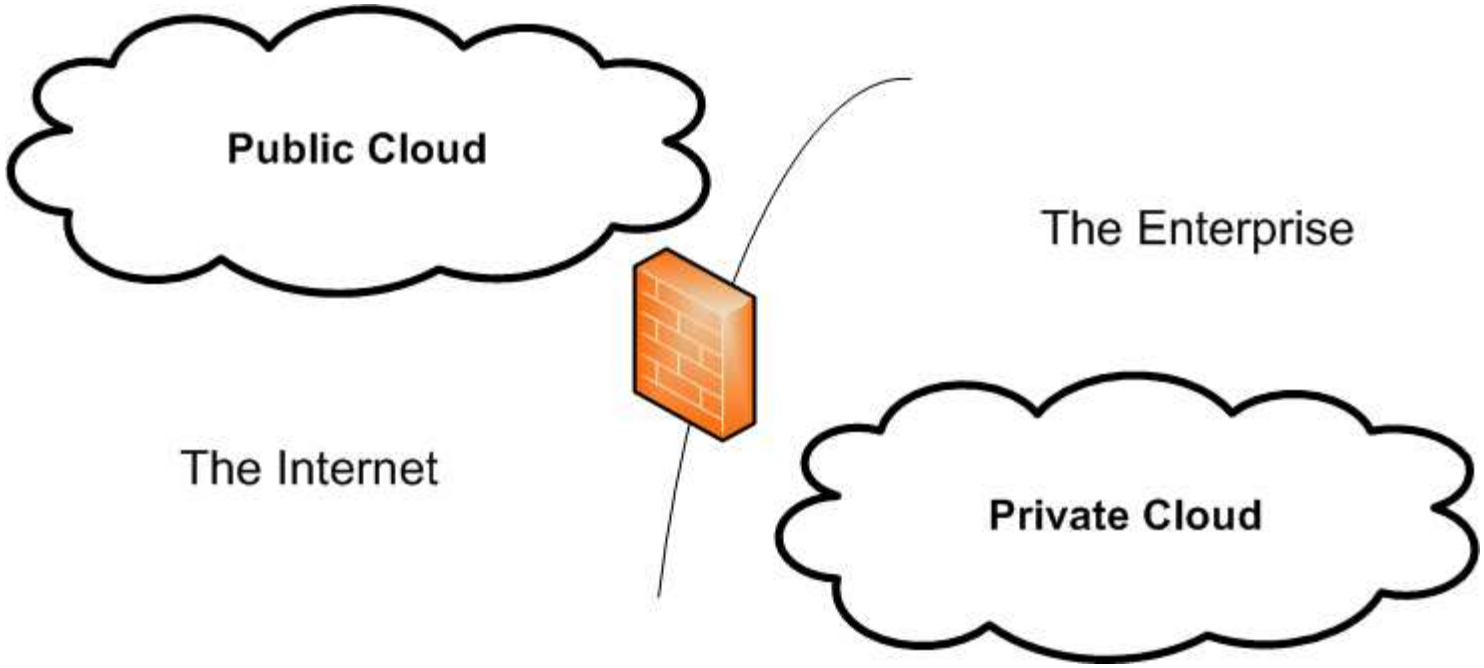
Variations on a Theme

- Public Cloud
- Private Cloud



Variations on a Theme

- Public Cloud
- Private Cloud
- Hybrid Cloud



Cloud computing risks and generic mitigation strategies

Areas of Risk

- Privileged User Access
- Data Segregation
- Regulatory Compliance
- Physical Location of Data
- Availability
- Recovery
- Investigative Support
- Viability and Longevity

Mitigation Strategies

- Understand the risks
- Evaluate any potential cloud-based solution and CSP
- Unique solution, generic risks

Risks

- Privileged User Access:
  - CSP must have access
  - Improper access -> Data Exposure
  - HR policies
  - 3rd party of a 3rd party

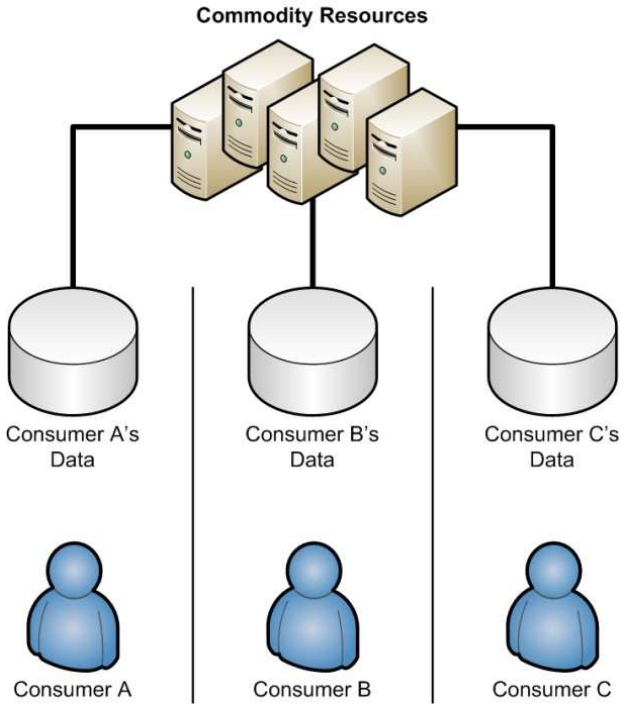
Mitigation

- Privileged User Access:
  - CSP must have access
  - Improper access -> Data Exposure
  - HR policies
  - 3rd party of a 3rd party

- Privilege Access Control Mitigation:
  - Support to HR and data policies
  - Outsourcing involved?
  - Evaluate the access controls

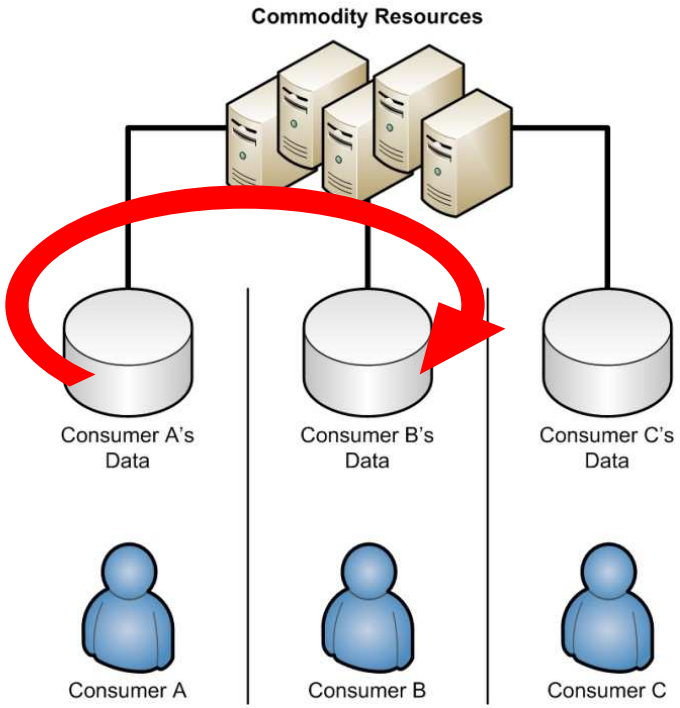
Risks

- Data Segregation:
  - Shared common resources
  - Multiple consumers, same physical machine
  - Failure to segregate data: data exposure, loss or corruption



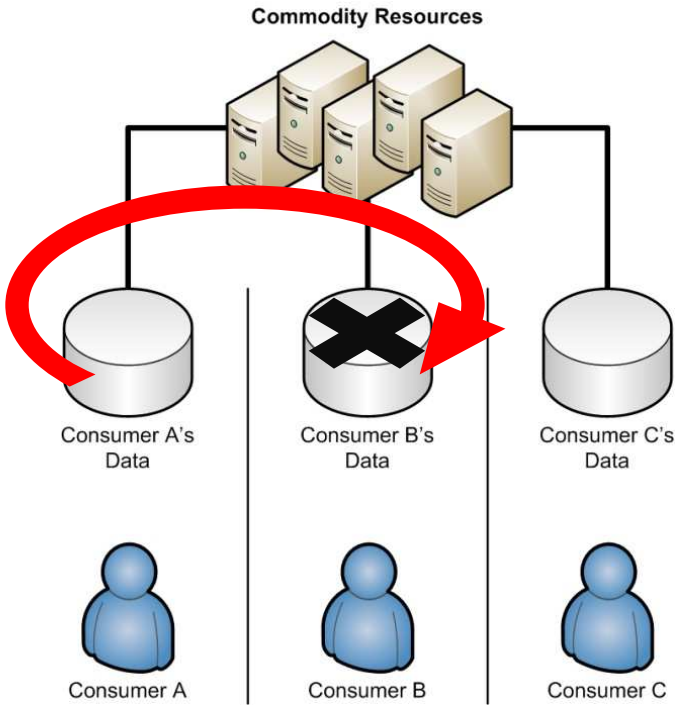
Risks

- Data Segregation:
  - Shared common resources
  - Multiple consumers, same physical machine
  - Failure to segregate data: data exposure, loss or corruption



Risks

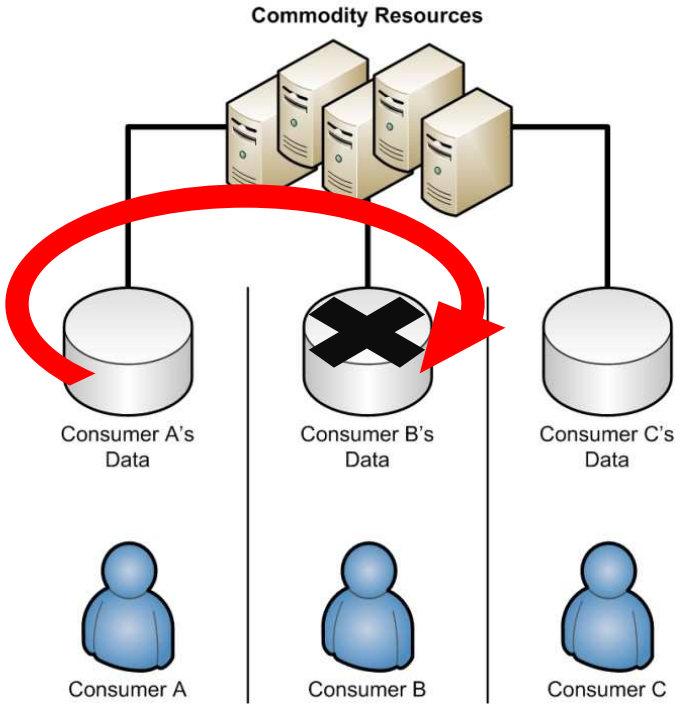
- Data Segregation:
  - Shared common resources
  - Multiple consumers, same physical machine
  - Failure to segregate data: data exposure, loss or corruption



Mitigation

- Data Segregation:
  - Shared common resources
  - Multiple consumers, same physical machine
  - Failure to segregate data: data exposure, loss or corruption

- Data Segregation Mitigation:
  - What's the risk of data segregation failure?
  - Encryption of data: shifting of risks
  - Understand the "how, where, when" of consumer data storage



Risks

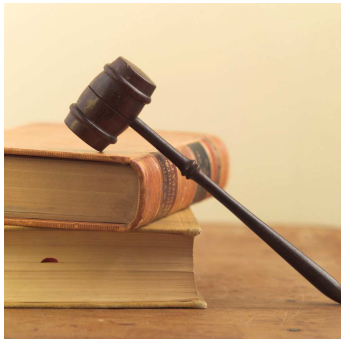
- Regulatory Compliance:
  - Regulations for sensitive information and outsourcing
  - Conflicting regulations and laws
  - Failure to comply: significant legal risks

Mitigation

- Regulatory Compliance:
  - Regulations for sensitive information and outsourcing
  - Conflicting regulations and laws
  - Failure to comply: significant legal risks

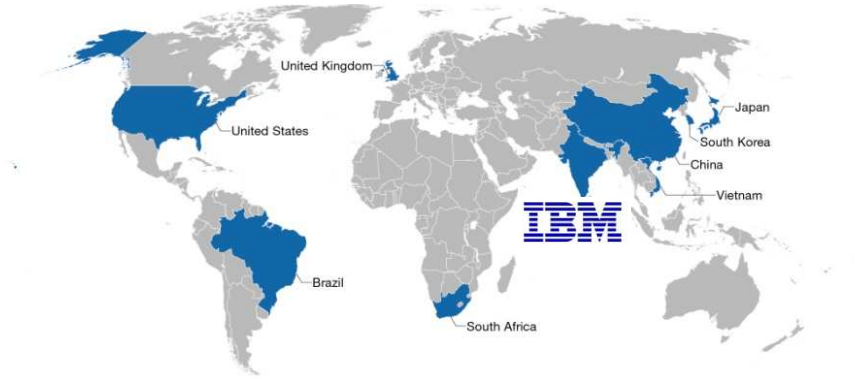
- Regulatory Control Mitigation:
  - Know your regulatory obligation
  - Know your CSP's regulatory obligations
  - Understand your liabilities
  - Location may change regulatory obligations

FISMA
HIPAA
SOX
PCI
SAS 70
Audits



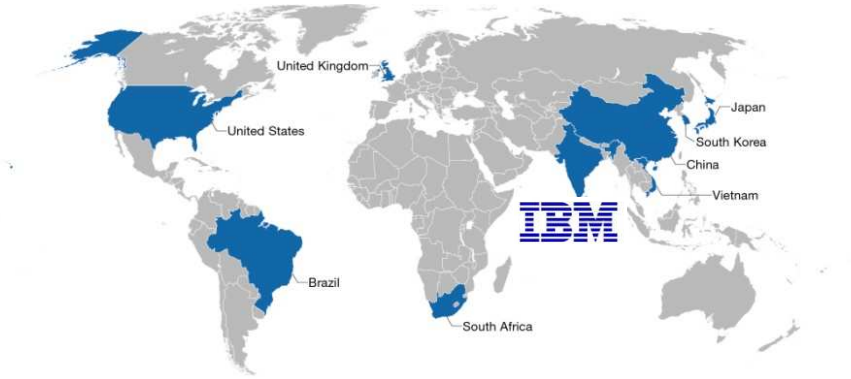
Risks

- Physical Location of Data:
  - Location, location, location
  - Location tied to regulatory issues
  - Volatile regions introduce a higher degree of risk
  - Hostile/Unethical governments have unforeseen risk of data exposure



Risks

- Physical Location of Data:
  - Location, location, location
  - Location tied to regulatory issues
  - Volatile regions introduce a higher degree of risk
  - Hostile/Unethical governments have unforeseen risk of data exposure



10/9/09

SA pigeon 'faster than broadband'

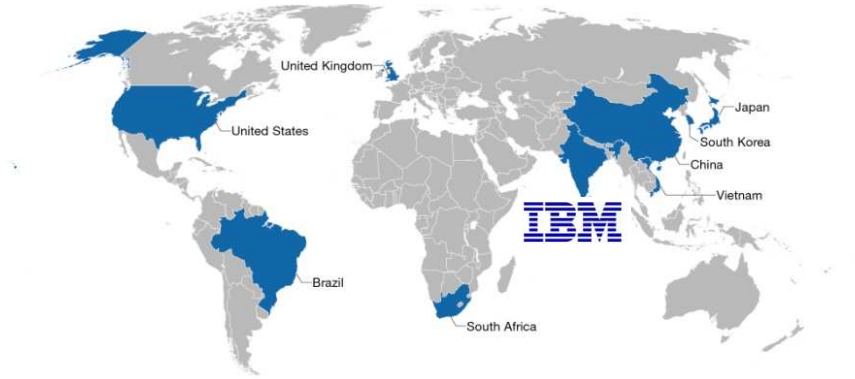
BBC News

Cyber A Durban IT company pitted an 11-month-old bird armed with a 4GB memory stick against the ADSL service from the country's biggest web firm, Telkom.

Winston the pigeon took two hours to carry the data 60 miles - in the same time the ADSL had sent 4% of the data. computers.

Mitigation

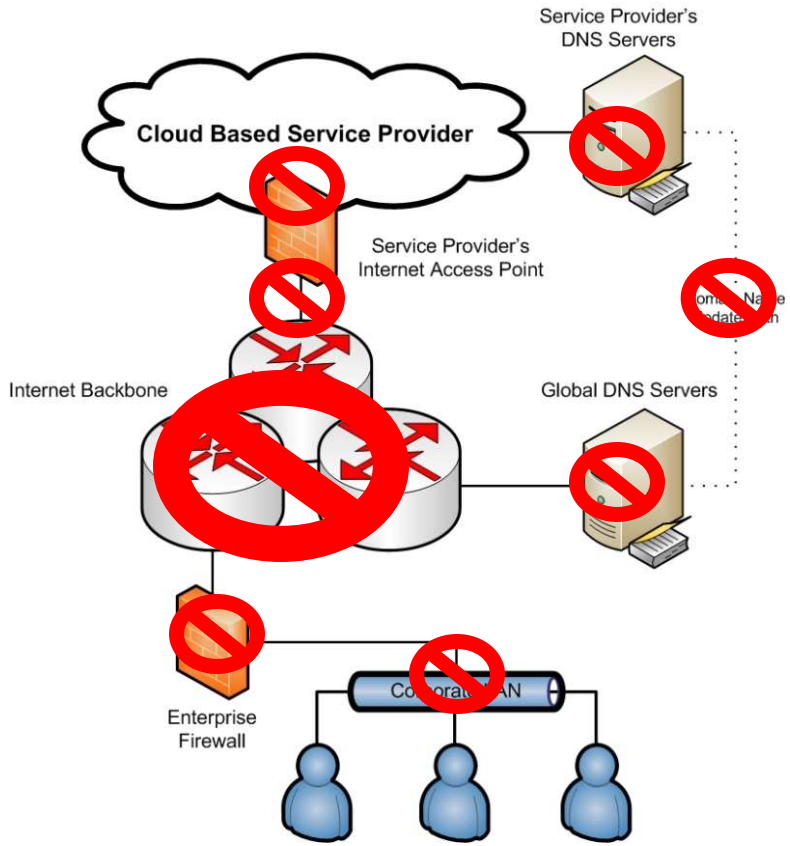
- Physical Location of Data:
  - Location, location, location
  - Location tied to regulatory issues
  - Volatile regions introduce a higher degree of risk
  - Hostile/Unethical governments have unforeseen risk of data exposure



- Physical Location of Data Mitigation:
  - Identify your data's location
  - Avoid CSPs that cannot guarantee the location
  - Avoid CSPs that use data centers in hostile countries
  - Use CSPs that reside in consumer's country

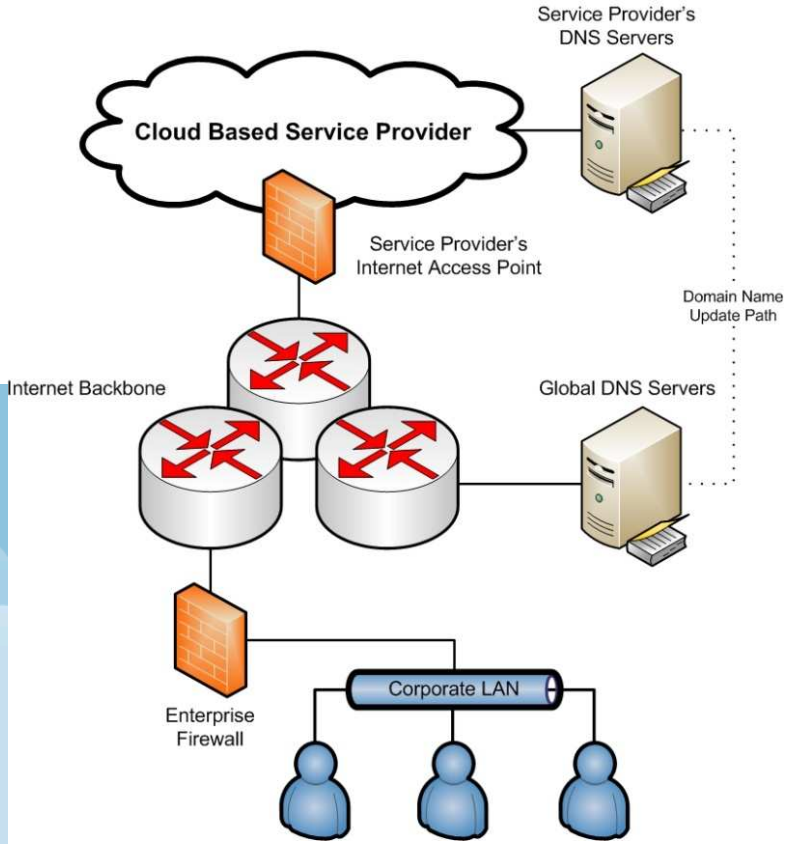
Risks

- Availability:
  - Constant connectivity required
  - Any failure terminating connectivity is a risk
  - Data loss and downtime risks



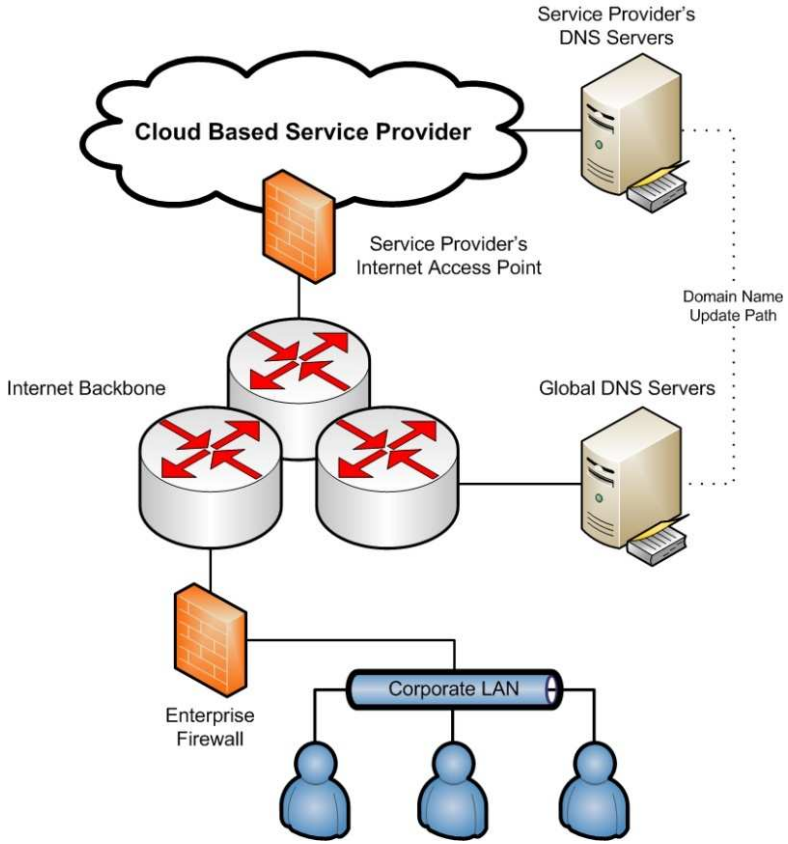
Risks

- Availability:
  - Constant connectivity required
  - Any failure terminating connectivity is a risk
  - Data loss and downtime risks



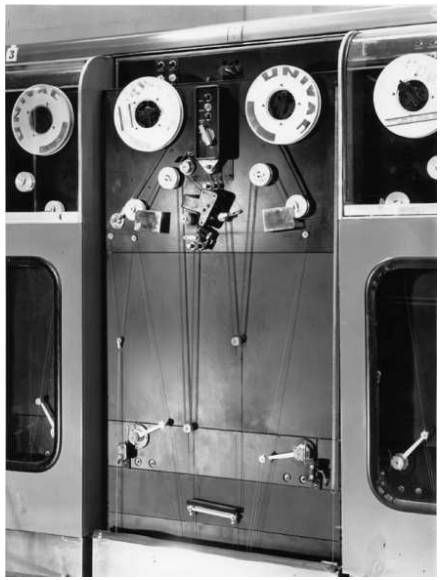
Mitigation

- Service Availability Mitigation:
  - Availability is the greatest risk !
  - Understand the CSP's infrastructure: avoid single points of failure
  - Private clouds may reduce the availability risk, but introduce additional cost and overhead
  - Establish service-level agreements (SLAs) with their CSPs
  - Balance the risk introduced by using multiple data centers with the risk of a single site failure
  - Assume at least one outage, what's the impact to you?



Risks

- Recovery:
  - Improper backups or system failure
  - The more data, more data loss risk
  - Recovery time is operational downtime

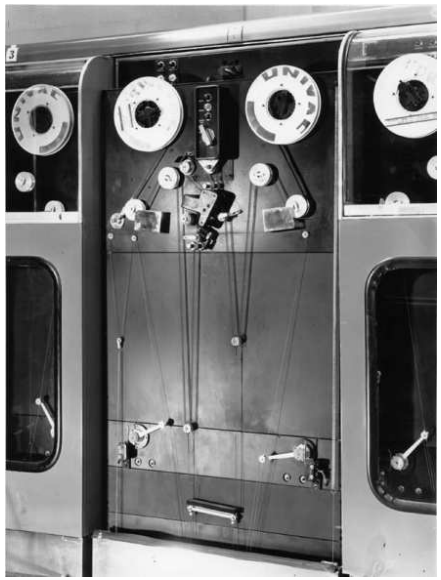


Mitigation

- Recovery:
  - Improper backups or system failure
  - The more data, more data loss risk
  - Recovery time is operational downtime

- Recovery Mitigation:
  - Understand backed up systems

    (Encrypted? Multiple sites?)
  - Identify the time required to completely recover data
  - Practice a full recovery to test the CSP's response time



Risks

- Investigative Support:
  - Multiple consumers, aggregated logs
  - CSPs may hinder incident responses
  - Uncooperative CSPs: lost forensic data and investigation hindrances

Mitigation

- Investigative Support:
  - Multiple consumers, aggregated logs
  - CSPs may hinder incident responses
  - Uncooperative CSPs: lost forensic data and investigation hindrances

- Investigative Support Mitigation:
  - Establish policies and procedures with the CSP
  - Avoid CSPs unwilling to participate in incident

Risks

- Viability and Longevity:
  - CSP failure can occur at any time, for any reason
  - Risk of data loss and operational downtime
  - Large companies sometimes terminate services
  - Abrupt shutdowns are a more significant risk

Mitigation

- Viability and Longevity:
  - CSP failure can occur at any time, for any reason
  - Risk of data loss and operational downtime
  - Large companies sometimes terminate services
  - Abrupt shutdowns are a more significant risk

- Viability and Longevity Mitigation:
  - Understand the way a CSP can “going dark”
  - Have a secondary CSP in mind
  - Review the history and financial stability of any CSP prior to engaging

Cloud Computing for Malicious Intent

Malicious use

- Bad guys are already using such technology **;)**
  - Botnets
  - Hacking as a Service, SPAM

Malicious use

- Bad guys are already using such technology
  - Botnets
  - Hacking as a Service, SPAM
- Malicious use of Cloud Services
  - C&C Server on the cloud
  - Storage of malicious data
  - Cracking passwords

11/9/09

Bot herders hide master control channel in Google cloud

by Dan Goodin, The Register

Cyber criminals' love affair with cloud computing just got steamier with the discovery that Google's AppEngine was tapped to act as the master control channel that feeds commands to large networks of infected computers.

Conclusion

Conclusions

- Understanding the risk of cloud-based solutions
- Understand the level of sensitivity of your data
- Perform due diligence when evaluating a CSP
- Identify the location of your data
- Get assurance that your data will remain where it is placed.

Cloud computing is a new technology still experiencing growing pains. Enterprises must be aware of this and anticipate the risks the technology introduces.

Additional Reading

- Cloud Security Alliance (CSA): “Security Guidance for Critical Areas of Focus in Cloud Computing”

  http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

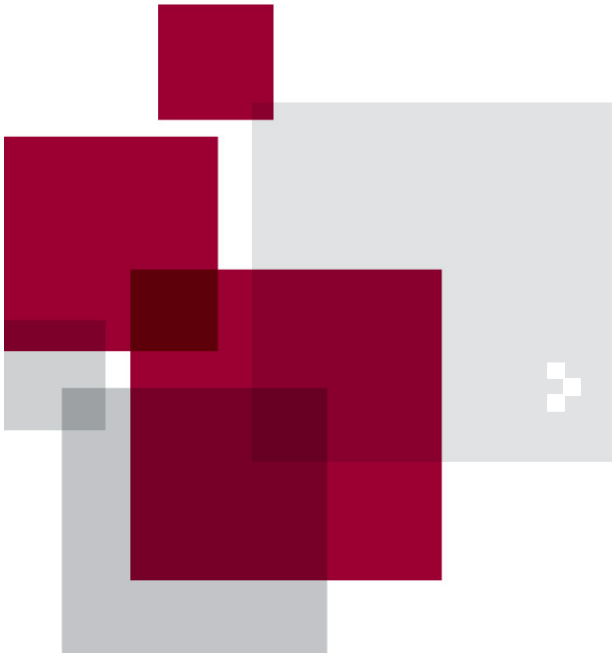
- NIST Cloud Computing Project

  http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

- ENISA report on “Cloud Computing: Benefits, risks and recommendations for information security”

  http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

- iDefense Topical Research Paper: “Cloud Computing”



Q&A

Thank You

Anchises M. G. de Paula
iDefense Intelligence Analyst
adepaula@verisign.com

iDEFENSE