



# Cloud Security: Are they really like oil and water?

Dr Paul Ashley  
IBM Security Solutions  
Australia Development Lab

## PulseANZ2010

Meet the people who can help  
advance your infrastructure



# Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© IBM Corporation 1994-2010. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at <http://www.ibm.com/legal/copytrade.shtml>.

## Outline

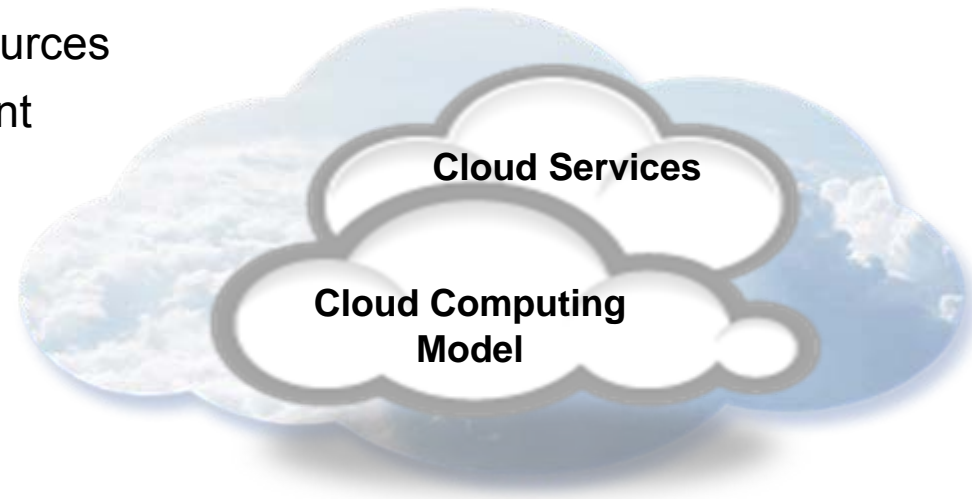
- Introduction to cloud computing
- Security in the cloud - what are the risks now and in the future?
- Guide to implementing a secure cloud



# Introduction to Cloud Computing

# Cloud: Consumption & Delivery Models Optimized by Workload

- “Cloud” is a **new consumption and delivery model** inspired by consumer Internet services.
- Enabled by
  - **Pooling and virtualization** of resources
  - **Automation** of service management
  - **Standardization** of workloads
- **Cloud enables:**
  - Self-service
  - Sourcing options
  - Flexible payment models
  - Economies-of-scale
- “Cloud” represents:
  - The **industrialization** of **delivery** for IT supported **services**



# Attributes and Benefits of Cloud Computing

VIRTUALIZATION

AUTOMATION

STANDARDIZATION

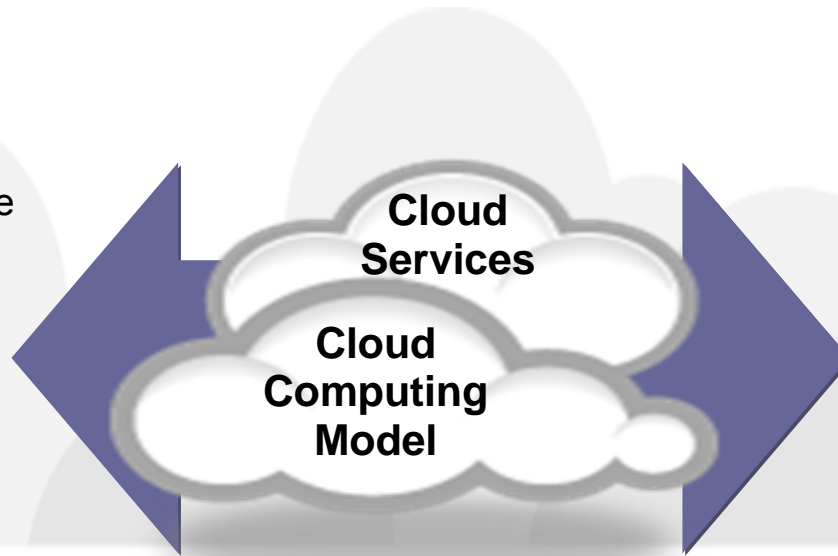
Attributes	Characteristics	Benefits
<b>Advanced virtualization</b>	IT resources can be shared between many applications. Applications can run virtually anywhere.	Providing more efficient utilization of IT resources. Reducing hardware cost through economy of scale
<b>Automated provisioning</b>	IT resources are rapidly provisioned or de-provisioned on demand.	Reducing IT cycle time (real-time provisioning) and management cost
<b>Elastic scaling</b>	IT environments scale down and up by large factors as the need changes.	Optimizing IT resources utilization Increasing flexibility
<b>Service catalog ordering</b>	Defined environments can be ordered from a catalog.	Enabling self-service, consumer concerns are abstracted from provider concerns through service interfaces
<b>Metering and billing Flexible pricing</b>	Services are tracked with usage metrics to enable multiple payment models.	Improving cost transparency Offering more flexible pricing schemes
<b>Internet Access</b>	Services are delivered through use of Internet.	Access anywhere, anytime

# Cloud Computing Delivery Models

## Private ...

- Access limited to enterprise and its partner network
- Dedicated resources
- Single tenant
- Drives efficiency, standardization and best practices while retaining greater customization and control
- Might be managed or hosted by third party

Customization, efficiency, availability, resiliency, security and privacy ...



## Hybrid ...

- Private infrastructure, integrated with public cloud

## Public ...

- Access open to everybody, subject to subscription
- Shared resources
- Multiple tenants
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis
- Always managed and hosted by 3<sup>rd</sup> party

Standardization, capital preservation, flexibility and time to deploy ...

# How far has your organisation progressed in Cloud Computing?

- A) No progress
- B) Implementing a Private Cloud
- C) Implementing a Public Cloud
- D) Implementing both Private and Public Clouds

**Text 0427 007 573**



# Westpac cautious on cloud computing

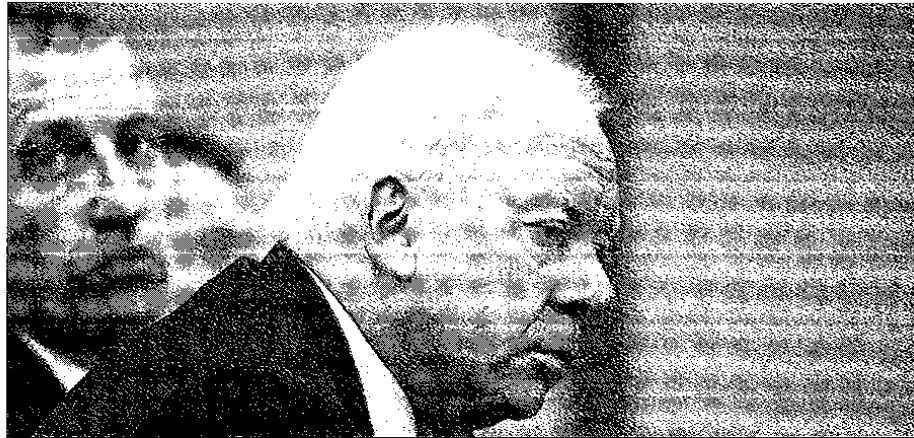
Julian Bajkowski

**W**estpac chief information officer Bob McKinnon has revealed the bank is aggressively pursuing the adoption of cloud computing technology in preparation for the end of its decade-long outsourcing contract with IBM, but future suppliers will be forced to provide any new services to the bank from within Australia.

Mr McKinnon told *The Australian Financial Review* that, owing to security concerns, the institution would require that all customer data that could be handled or processed by external parties would need to remain onshore, the strongest statement on the issue of data sovereignty to date by a local institution.

"Customer data is very sensitive and the last thing people want is their data turning up in a different jurisdiction where there may or may not be the same amount of controls around [data security that exist in Australia]," Mr McKinnon said. "Offshore you lose control of that. We feel we are in a much better position to protect both our data and our customers' data if it's in our own secure perimeter."

Mr McKinnon's tough stand on data security is likely to act as a reference point for local institutions as they look for ways to cut costs by



**Bob McKinnon: 'We are in a much better position to protect our data if it's in our own secure perimeter.'** Photo: ROB HOMER

upgrading legacy technology systems.

Westpac is heading into the final leg of negotiations with suppliers over how it will buy future computing infrastructure services to replace one of the three biggest outsourcing deals yet struck in Australia.

The break-up of the \$4.3 billion IBM contract is regarded as a potential catalyst for Westpac to drive big efficiencies over and above those set out under its \$700 million integration plan with St George,

which has already resulted in the rationalisation of general ledger and human resources applications.

Cloud computing allows businesses to buy their processing power on-demand on a pricing regime similar to utility services such as power and water.

The technology's primary appeal is that it dramatically lifts infrastructure capacity utilisation and allows for greater flexibility in allocating resources while shedding the high capital cost of running systems in-house.

Mr McKinnon said a similar flexibility to that offered by offshore cloud suppliers could be obtained by applying the same virtualisation technology to locally run machines.

"When we look at cloud computing, we look at it as an opportunity for us to get better value out of virtualisation technology, but in our own private way," Mr McKinnon said. "We've got the scale as an organisation to build private clouds."

However, he cautioned that big enterprise application vendors would

## KEY POINTS

- Westpac will require that all customer data handled by third parties stays onshore.
- It sees opportunities in cloud computing but has the capacity to build private clouds.

move to a software-as-a-service model soon. "There is no way we could buy most of the things we need to run our bank as a service from somebody else," Mr McKinnon said.

In its interim results presentation last week, Westpac said it was on track with seven out of 13 key technology projects in a bank-wide systems overhaul it claims will put it on par with rival Commonwealth Bank of Australia.

Among projects on the boil are moves to modernise its core payments infrastructure by building a new platform for card origination and servicing. Enterprise payment systems are also being consolidated onto a single platform for clearing, settlements and automatic teller and Eftpos switching.

Westpac's financial statements list the migration of key "products and accounts" onto the Hogan core banking platform as in "preliminary planning" but note that the move will see 19 other systems shut down.

The migration to the Hogan system "will enable real time banking for Westpac", the notes said.

# Workloads Most Considered for Cloud Delivery

## Top public workloads

- Audio/video/Web conferencing
- Service help desk
- Infrastructure for training and demonstration
- WAN capacity and VoIP infrastructure
- Desktop
- Test environment infrastructure
- Storage
- Data center network capacity
- Server

*Infrastructure and collaboration workloads emerge as most appropriate*

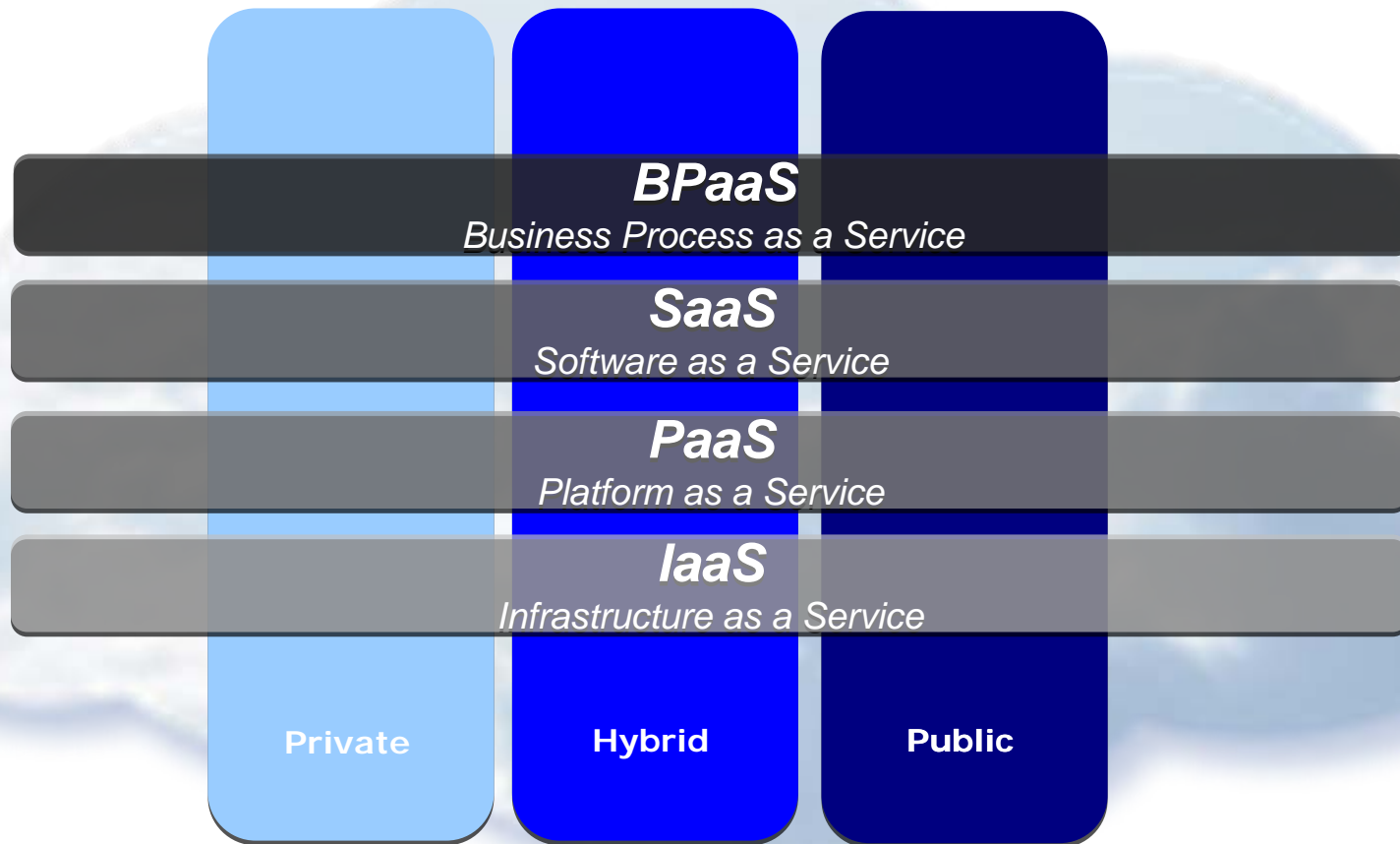
## Top private workloads

- Data mining, text mining, or other analytics
- Security
- Data warehouses or data marts
- Business continuity and disaster recovery
- Long-term data archiving/preservation
- Transactional databases
- Industry-specific applications
- ERP applications

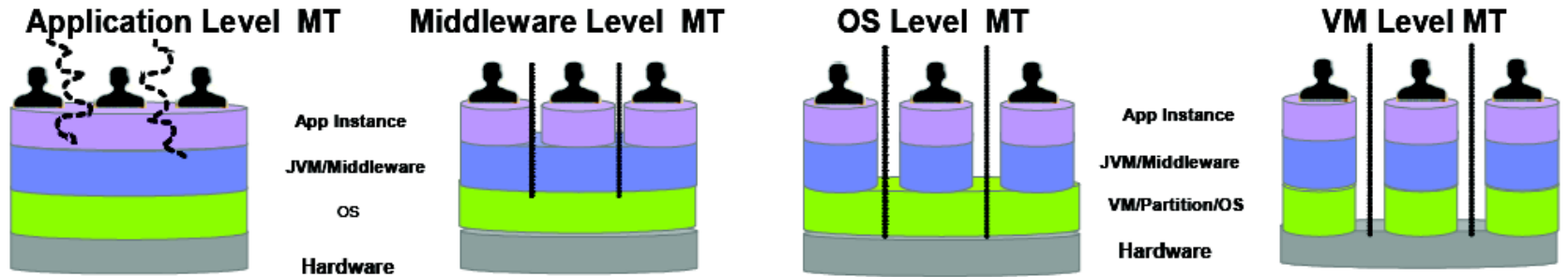
*Database and application workloads emerge as most appropriate*

Source: IBM Market Insights, *Cloud Computing Research*, July 2009. n=1,090

# So, what are the different Cloud Computing models?

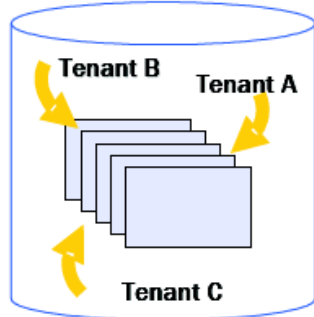


# What is multi-tenancy, and what are the security IMPLICATIONS?

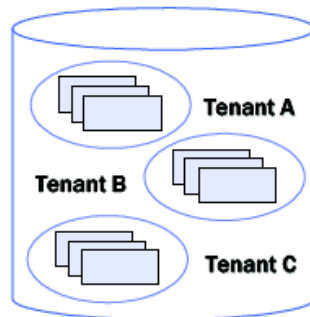


## Example: Database Multi-tenancy

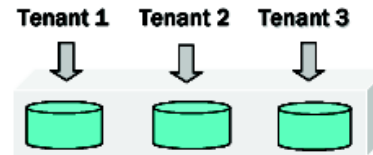
Same Table, hidden tenant ID field



Same DB, separate tables or schemas



Same server, separate DB



Separate DB servers (instances)



# From a security point of view, what type of multi-tenancy public approach would you be most comfortable with?

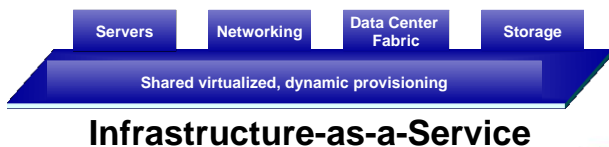
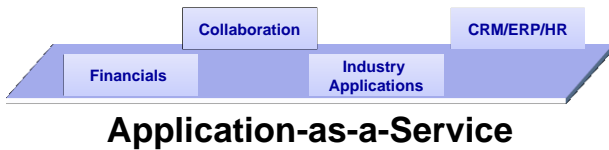
- A) Application Level
- B) Middleware Level
- C) Operating System Level
- D) Virtual Server Level

**Text 0427 007 573**

# Information security is BOTH the responsibility of the provider and the consumer

Who is responsible for security at the ... level?

*Datacenter Infrastructure Middleware Application Process*



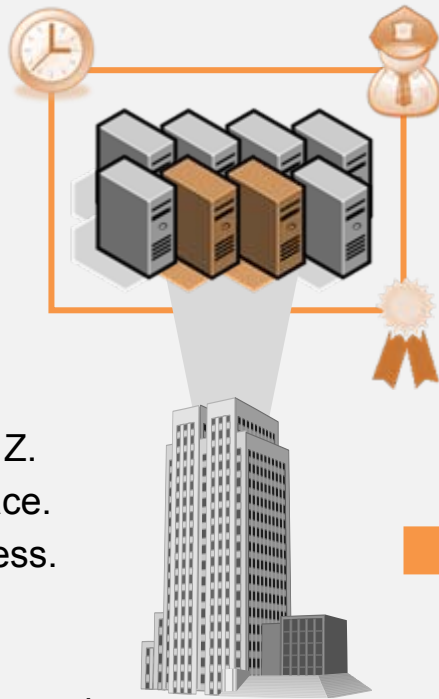


# Security in the cloud - what are the risks now and in the future?



# Simple Example

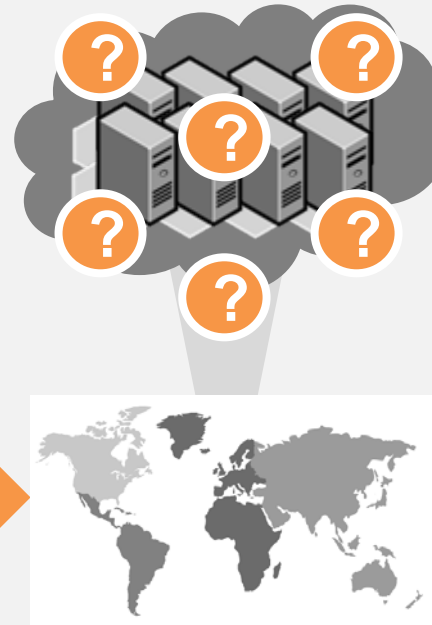
## Today's Data Center



### We Have Control

It's located at X.  
It's stored in server's Y, Z.  
We have backups in place.  
Our admins control access.  
Our uptime is sufficient.  
The auditors are happy.  
Our security team is engaged.

## Tomorrow's Public Cloud



### Who Has Control?

Where is it located?  
Where is it stored?  
Who backs it up?  
Who has access?  
How resilient is it?  
How do auditors observe?  
How does our security team engage?



# Security Remains the Top Concern for Cloud Adoption

## 80%

Of enterprises consider security the #1 inhibitor to cloud adoptions

## 48%

Of enterprises are concerned about the reliability of clouds

## 33%

Of respondents are concerned with cloud interfering with their ability to comply with regulations

*“How can we be assured that our data will not be leaked and that the vendors have the technology and the governance to control its employees from stealing data?”*

*“Security is the biggest concern. I don’t worry much about the other “-ities” – reliability, availability, etc.”*

*“I prefer internal cloud to IaaS. When the service is kept internally, I am more comfortable with the security that it offers.”*

Source: Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman)

# Specific Customer Concerns Related to Security

Protection of intellectual property and <u>data</u>	30%
Ability to enforce regulatory or contractual obligations	21%
Unauthorized use of <u>data</u>	15%
Confidentiality of <u>data</u>	12%
Availability of <u>data</u>	9%
Integrity of <u>data</u>	8%
Ability to test or audit a provider's environment	6%
Other	3%

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey

# Categories of Cloud Computing Risks

## Control

Many companies and governments are uncomfortable with the idea of their information located on systems they do not control.

**Providers must offer a high degree of security transparency to help put customers at ease.**

## Data

Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure.

**Authentication and access technologies become increasingly important.**

## Reliability

High availability will be a key concern. IT departments will worry about a loss of service should outages occur.

**Mission critical applications may not run in the cloud without strong availability guarantees.**

## Compliance

Complying with regulations may prohibit the use of clouds for some applications.

**Comprehensive auditing capabilities are essential.**

## Security Management

Even the simplest of tasks may be behind layers of abstraction or performed by someone else.

**Providers must supply easy controls to manage security settings for application and runtime environments.**

# What type of data would you be comfortable sending to a public cloud?

- A) Only public information
- B) Organisational email and file backups
- C) Personally Identifiable Information (PII)
- D) Mission Critical

**Text 0427 007 573**

- IEEE Spectrum
- April 2010

# Too Big to Hack

To keep cyberspace secure, must governments regulate mighty Google?

**E**ARLY THIS YEAR, when the search giant Google fell victim to hackers in China, a lot of wild-eyed speculation began. Will Google carry out its threat to pull out of China? Could Google, like Microsoft before it, face crippling antitrust lawsuits? Might the company end up a semiregulated public utility? And, given the monopoly status of such a utility, would Google quietly enjoy such a future?

Probably not, maybe, no, and no, say cybersecurity and antitrust experts.

It all began in January, when Google said it had recently detected hacks


digging into and getting the source code for Google's intellectual property."

The problem goes far beyond the Chinese market, Payne says. The hack undercut the trust necessary for the adoption of all of Google's applications, notably e-mail, word processing, spreadsheets, and now social networking. One large financial service organization, the name of which Payne declined to provide, had been planning to shift more of its IT infrastructure over to Google apps. But, "when this [Google hack] happened, they immediately started reevaluating," he says.

Mark Kadrich, CEO of consulting firm The Security Consortium, in San Jose, Calif., says he thinks the attack was at its core about market share.

"My hunch is this attack directly targeted intellectual property Google has—to help Baidu be more competitive," says Kadrich. Baidu is a search engine based in China.

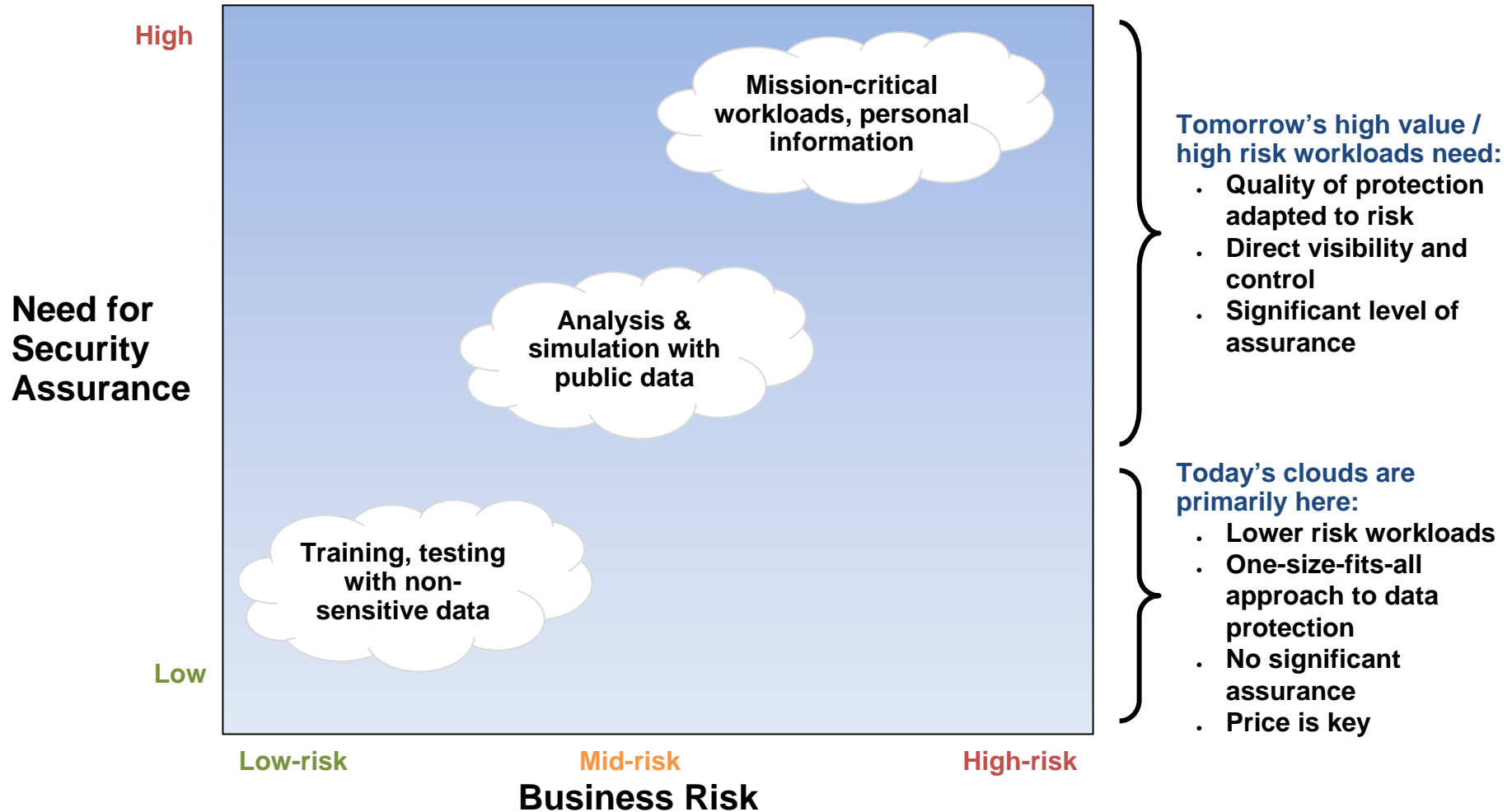
Google has turned to spy agencies like the National Security Agency, not as



# Guide to implementing a secure cloud

# One-size does not fit-all

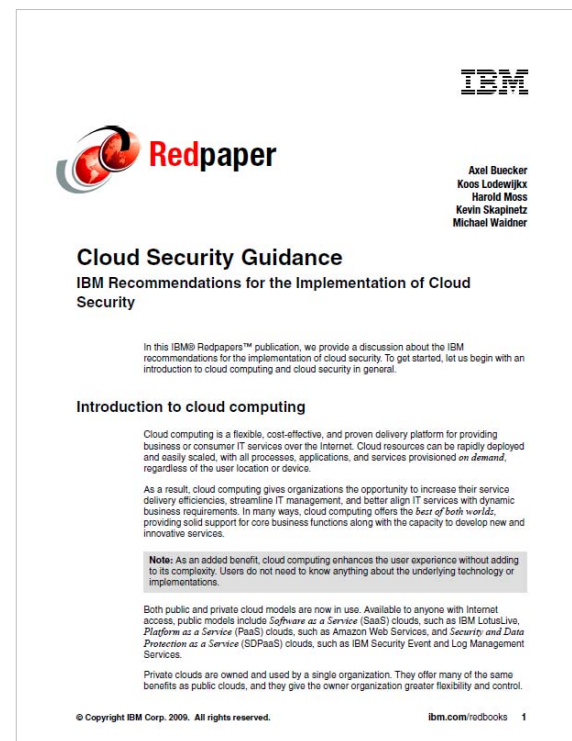
Different cloud workloads have different risk profiles



# IBM Cloud Security Guidance document

- Based on cross-IBM research on cloud security
- Highlights a series of best practice controls that should be implemented
- Broken into 7 critical infrastructure components:

- *Building a Security Program*
- *Confidential Data Protection*
- *Implementing Strong Access and Identity*
- *Application Provisioning and De-provisioning*
- *Governance Audit Management*
- *Vulnerability Management*
- *Testing and Validation*







IBM Security Framework



IBM Cloud Security Guidance Document

## Security governance, risk management and compliance

**Customers require visibility into the security posture of their cloud.**

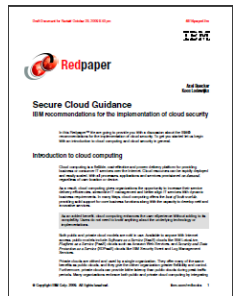
### Implement a governance and audit management program

Establish 3rd-party audits (ISO27001, PCI)

- Provide access to tenant-specific log and audit data
- Create effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- Create policies for PII and for data crossing International boundaries
- Understand applicable regional, national and international laws
- Support for forensics and e-Discovery



IBM Security Framework



IBM Cloud Security Guidance Document

## People and Identity

**Customers require proper authentication of cloud users.**

### Implement strong identity and access management

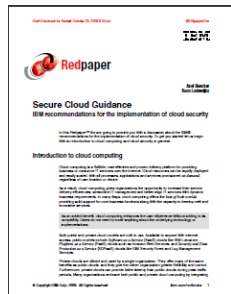
- Implement least privilege model for user's access
- Strong Identity lifecycle management
- All administrative access over secure channels
- Privileged user monitoring, including logging activities, physical monitoring and background checking
- Utilize federated identity to coordinate authentication and authorization with enterprise or third party systems
- A standards-based, single sign-on capability



IBM Security Framework

## Data and Information

**Customers cite data protection as their most important concern.**



IBM Cloud Security Guidance Document

### Ensure confidential data protection

- Protect PII and Intellectual Property
- Implement a secure key management program
- Use a secure network protocol when connecting to a secure information store.
- Implement a firewall to isolate confidential information, and ensure that all confidential information is stored behind the firewall.
- Sensitive information not essential to the business should be securely destroyed.



IBM Security Framework



IBM Cloud Security Guidance Document

## Application and Process

**Customers require secure cloud applications and provider processes.**

### Establish application and environment provisioning

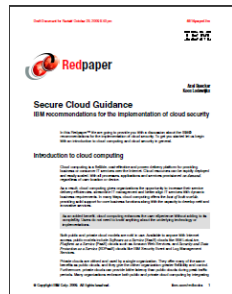
- Implement a program for application and image provisioning.
- Ensure provisioning management is strictly controlled
- Protect machine images from corruption and abuse
- Ensure all changes to virtual images and applications are logged.
- Ensure provisioned images apply appropriate access rights
- Ensure destruction of outdated images



IBM Security Framework

## Network, Server and End Point

**Customers expect a secure cloud operating environment.**



IBM Cloud Security Guidance Document

## Maintain environment testing and vulnerability/intrusion management

- Implement vulnerability scanning, anti-virus, intrusion detection and prevention on all appropriate images
- Ensure isolation exists between tenant domains
- Trusted virtual domains: policy-based security zones
- A secure application testing program should be implemented.
- Develop all Web based applications using secure coding guidelines.
- Ensure external facing Web applications are black box tested



IBM Security Framework



IBM Cloud Security Guidance Document

## Physical Security

**Customers expect cloud data centers to be physically secure.**

### Implement a physical environment security plan

- Ensure the facility has appropriate controls to monitor access.
- Prevent unauthorized entrance to critical areas within facilities e.g. servers, routers, storage, power supplies
- Biometric access of employees
- Ensure that all employees with direct access to systems have full background checks.
- Provide adequate protection against natural disasters.

## Summary

- “Cloud” is a new consumption and delivery model inspired by consumer Internet services.
- Security Remains the Top Concern for Cloud Adoption
- One sized security doesn't fit all
- Take a structured approach to securing your cloud environment
- Documented guidance is available for download to assist you in securing your cloud environment



**Thank you!**

**For more information, please visit:**

[ibm.com/cloud](http://ibm.com/cloud)

[ibm.com/security](http://ibm.com/security)