mobile business

Guest Lecture 3

Cloud Computing

Mobile Business II (SS 2016)

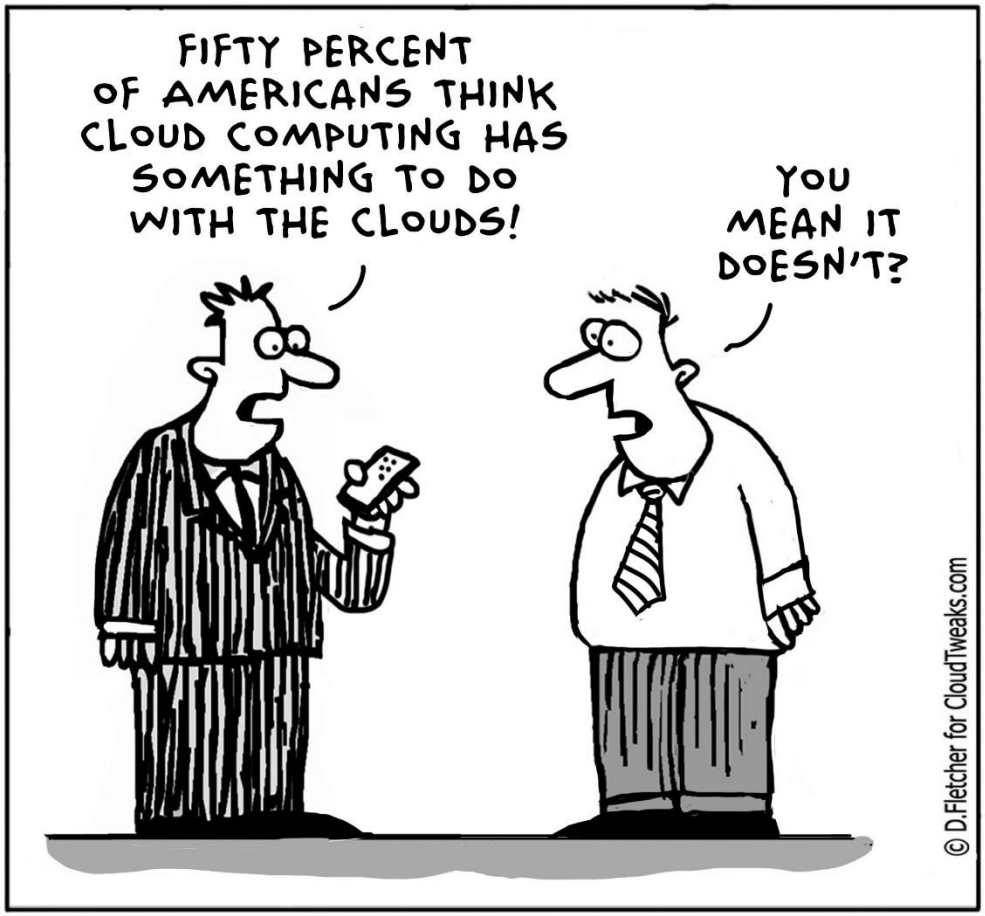
Dr. Sebastian Pape
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt a. M.

mobile business

Agenda

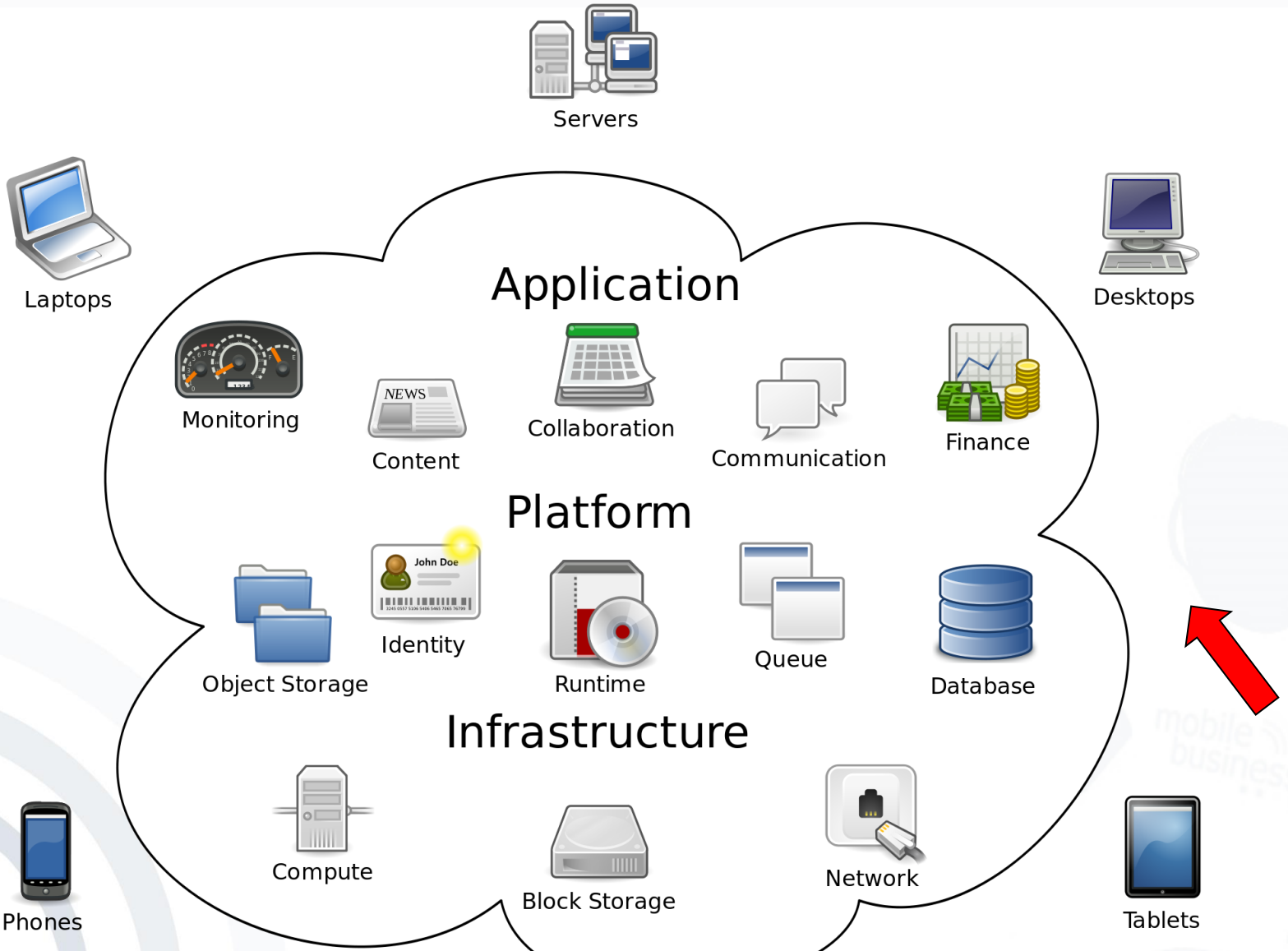
- What is Cloud Computing
  - Terminology
- What is Cloud Computing used for
- Cloud Security
- Cloud Provider Selection

What is Cloud Computing?



[Source: Fletcher, 2012]

What Is Cloud Computing?



[Source: Johnston, 2009]

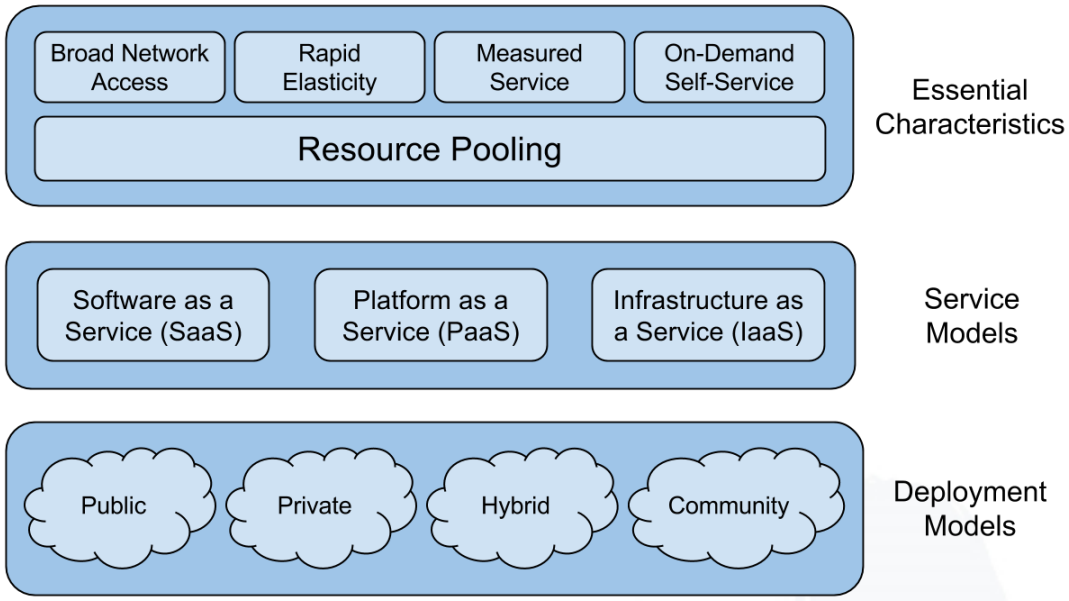
NIST Definition

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- This cloud model is composed of five essential characteristics, three service models, and four deployment models.

NIST Definition II

- New way of delivering computing resources
- Shared among different consumers (**Resource Pooling**)
- Available when needed (**On-Demand Self-Service**)
- Accessible through a **network**
- Scale in/scale out (**Rapid Elasticity**)
- Control/Optimize Usage (**Measured Service**)



NIST Definition of Cloud Computing

Terminology

[Source: Fletcher, 2012]

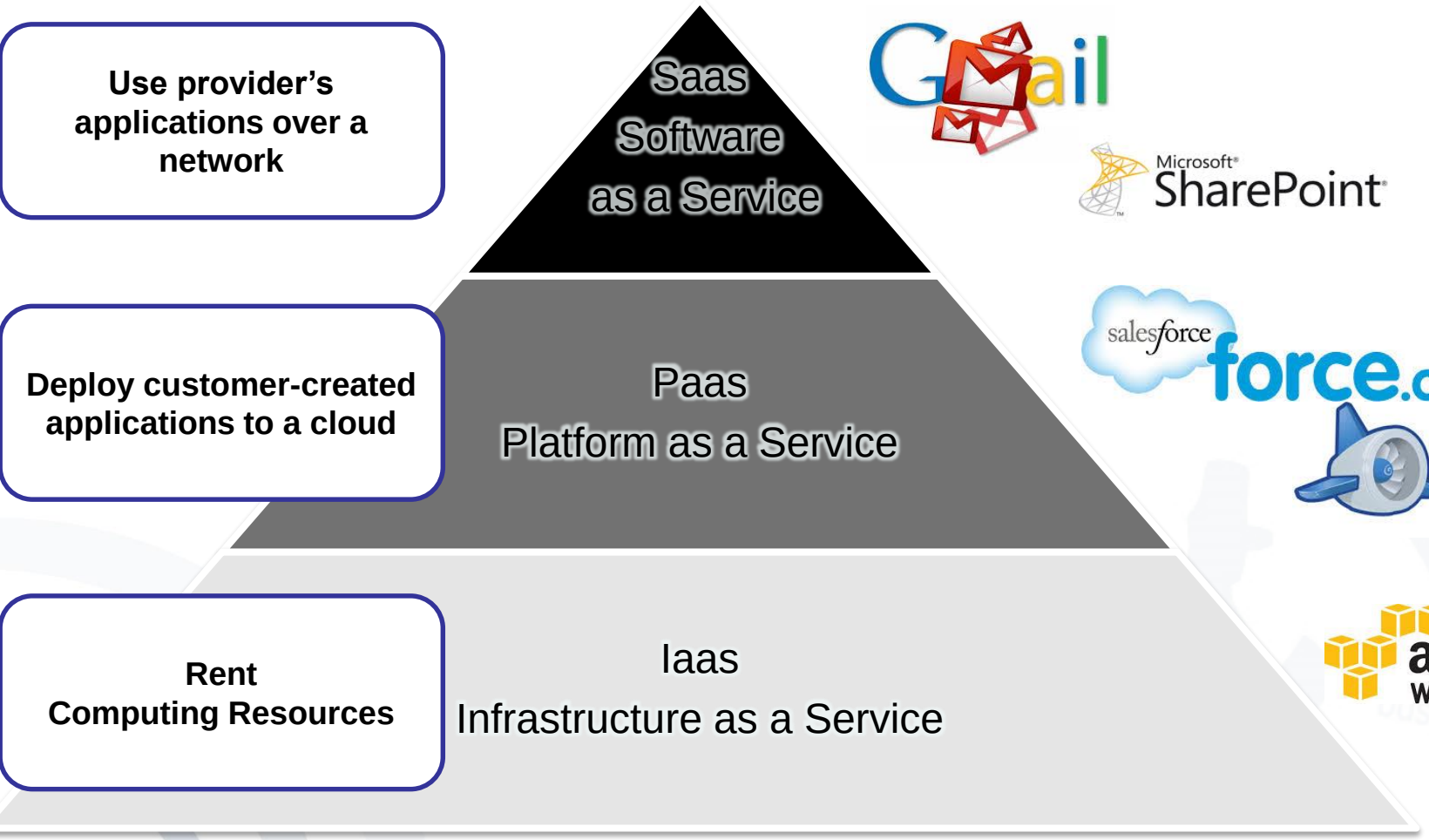
mobile business

Cloud Service Models

Use provider's applications over a network

Deploy customer-created applications to a cloud

Rent Computing Resources



Gmail

Microsoft SharePoint

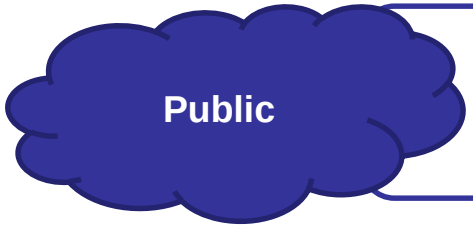
salesforce force.com

Google App Engine

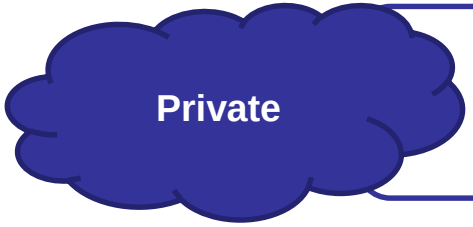
amazon web services™

mobile business

Cloud Deployment Models

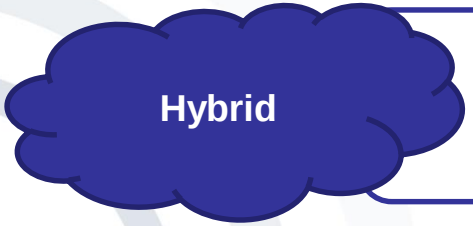


- Cloud Platform for use by general public
- Externally hosted by Cloud Provider



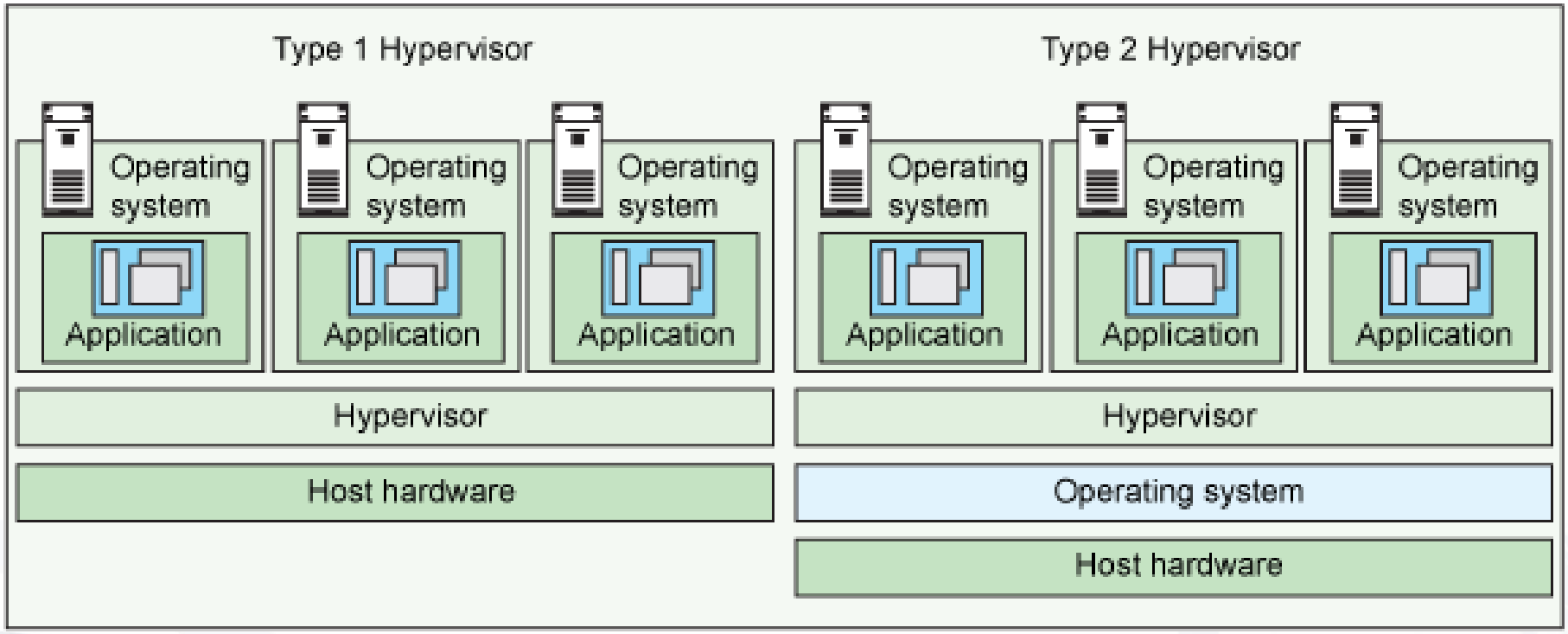
- Cloud Platform for use by one organization
- Can be externally or internally hosted

- Cloud Platform shared by several organizations
- Can be externally or internally hosted



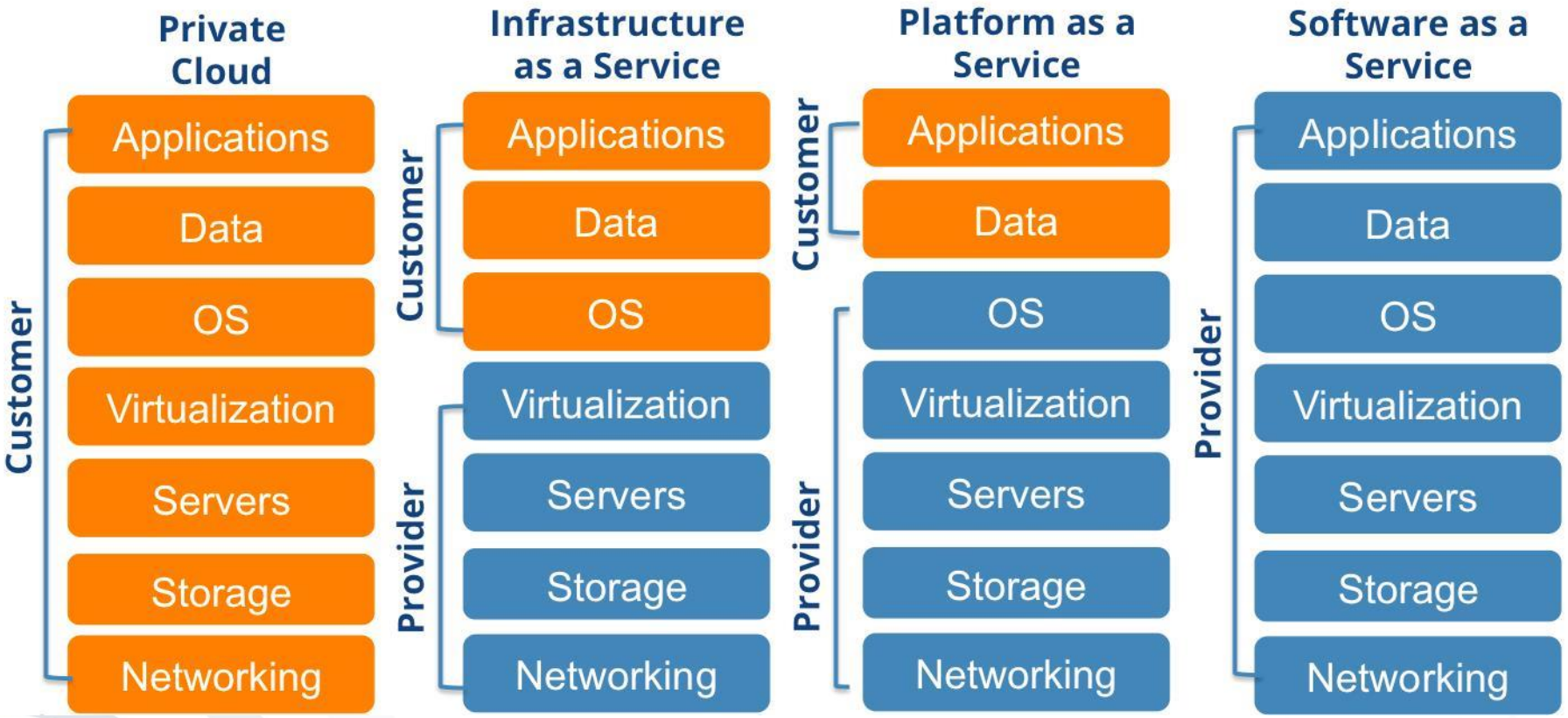
- A combination of the clouds above

Technical Background: Virtualisation



- **Virtualisation is not a requirement for Cloud Computing**
- **But the majority of providers make use of it since it makes resource pooling / elasticity easier**

Levels of Control

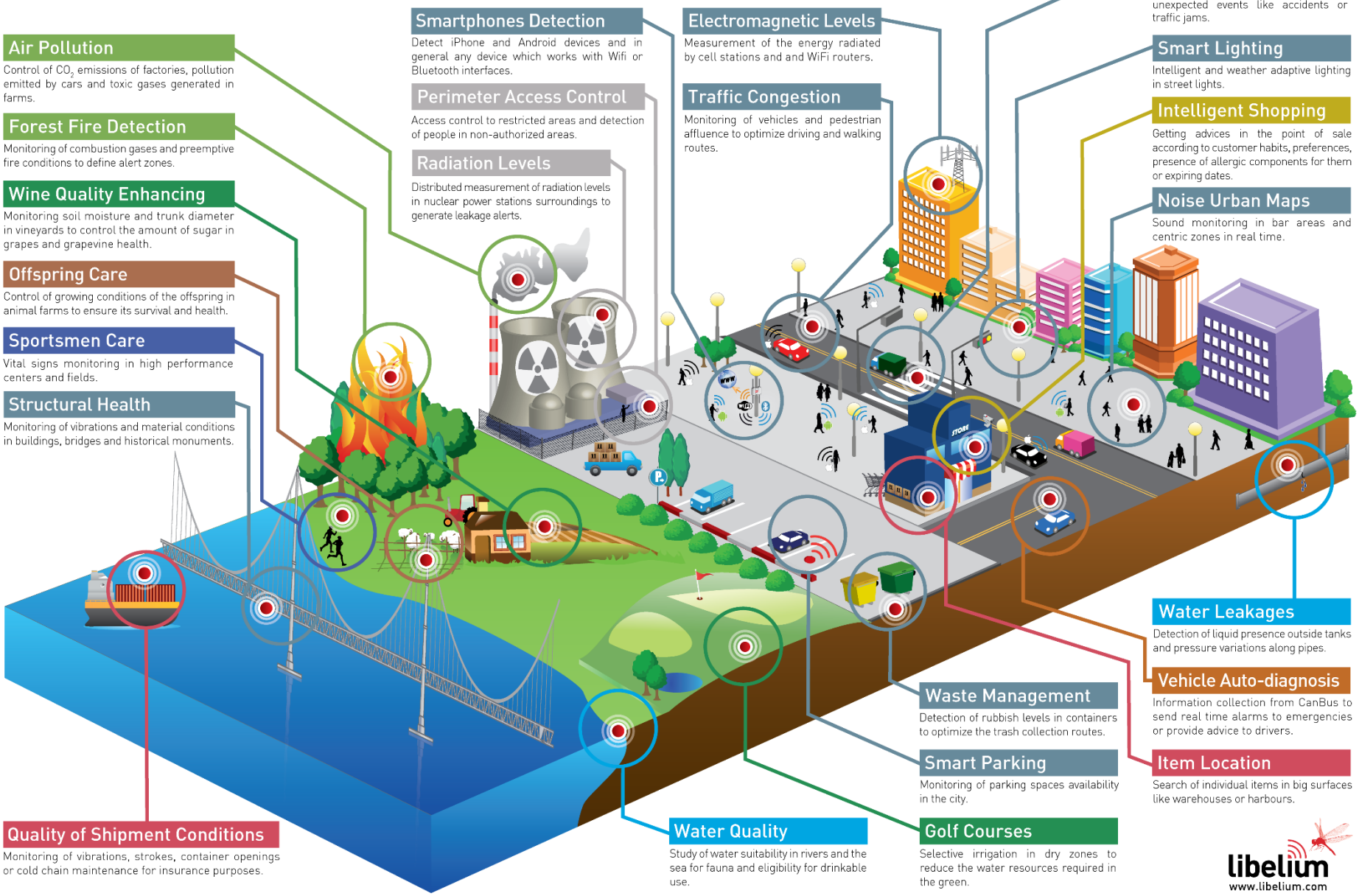


[Source: SevOne, 2014]

What is Cloud Computing used for?

[Source: Fletcher, 2012]

Libelium Smart World



Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.

Sportsmen Care
Vital signs monitoring in high performance centers and fields.

Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.

Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.

Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Electromagnetic Levels
Measurement of the energy radiated by cell stations and and WiFi routers.

Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.

Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.

Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.

Smart Roads
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Smart Lighting
Intelligent and weather adaptive lighting in street lights.

Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.

Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.

Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.

Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.

Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.

Smart Parking
Monitoring of parking spaces availability in the city.

Item Location
Search of individual items in big surfaces like warehouses or harbours.

libelium
www.libelium.com

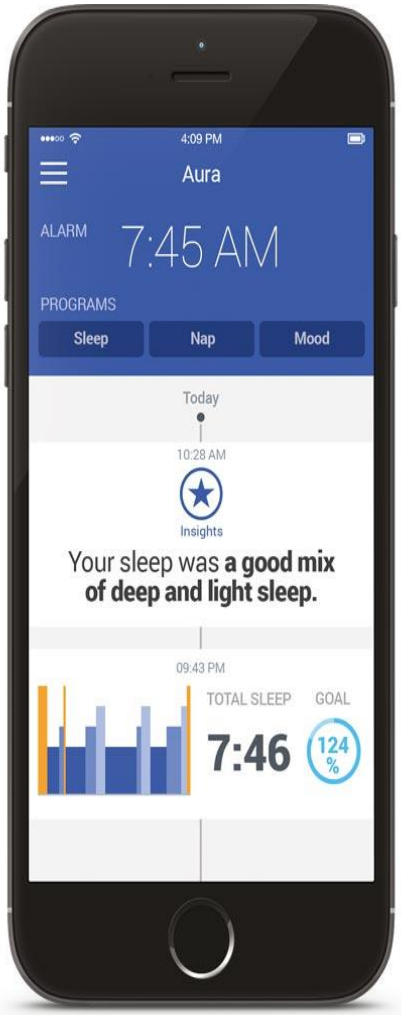
[Source: Forbes.com]

mobile business

Internet of Things: Coffe maker

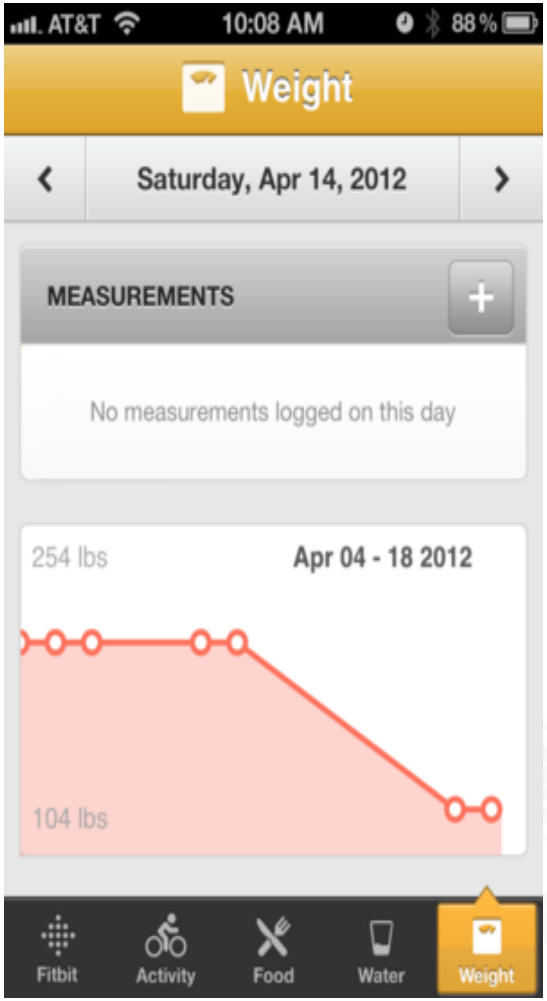
[Philipps / Saeco]

Internet of Things: Health Care



[Withings]

Internet of Things: Health Care II



[Fitbit]

mobile business

Internet of Things: More devices

[Sony]

[Linksys]

[Mattel]

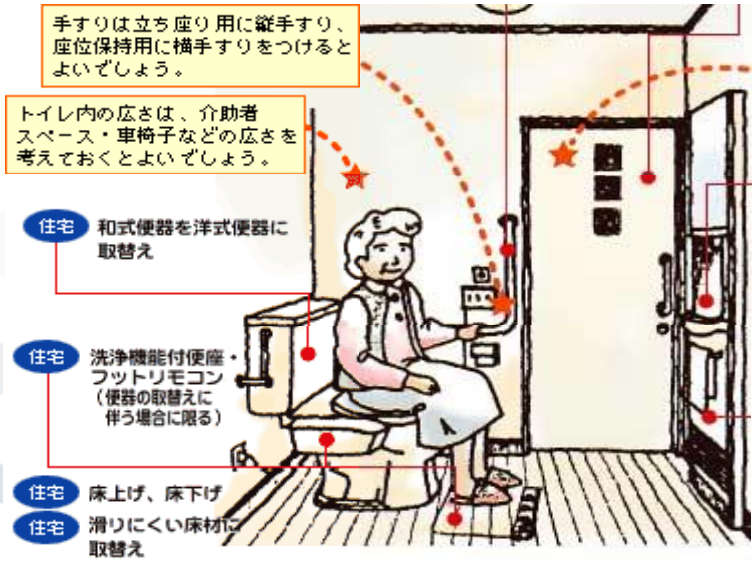
[LG]

[Beurer]

[Source: Discovergy]

The networked washlet

- … and in Japan, Matsushita has demonstrated a health-monitoring toilet that can analyze your stool and send the information online to your doctor. [www.asiaweek.com/asiaweek/technology/article/0,8707,130495,00.html, 2001-06-22]
- “ … sensors detect seven abnormal behavior patterns of the elderly in their living quarters and three abnormal patterns in the toilet area. Any abnormality that is sensed is automatically transmitted to the PHS terminals or pagers of the nursing staff. The care monitor system that uses these sensors will help provide safe and high quality nursing service.” [www.mew.co.jp/e-tecrepo/73e/main02.html]



[Hitachi, Matsuhita Electric Works Limited, Panasonic, Toto]

Smart Home Devices in general

- Massively networked
- In most cases controlled via apps
- Specialised to one application

- Data often stored in the cloud / with 3rd parties
  - Access via provider's server
  - Globally distributed
- In most cases app und device come from the same provider – but sometimes 3rd parties are involved.

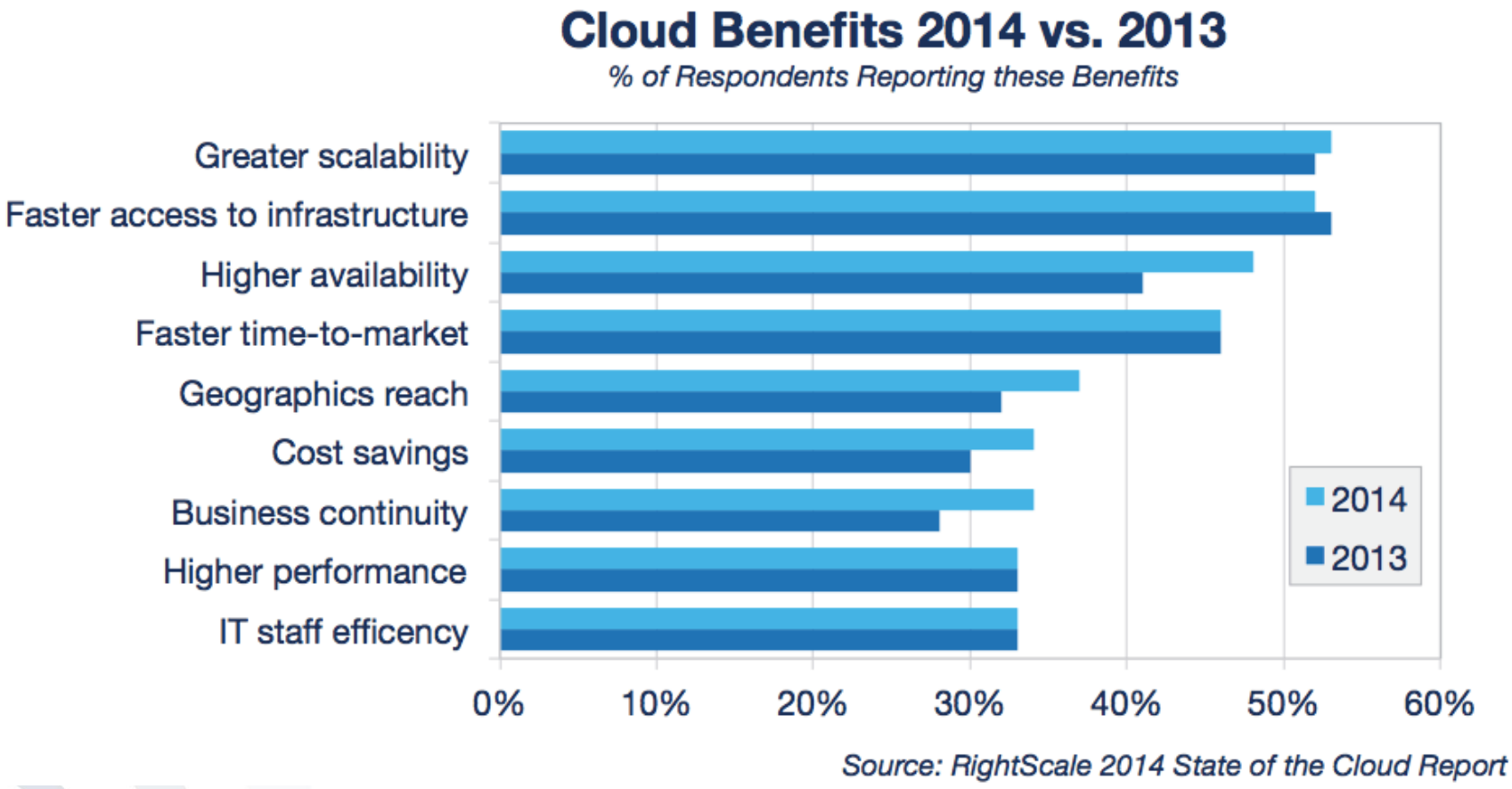
- Privacy terms lengthy and/or difficult to understand

Why using Cloud Computing?

- **Benefits of Cloud**
  - Cost Effectiveness
  - Flexibility
  - Scalability and Elasticity
  - Quick Deployment
  - Ubiquitous Access to Computing Resources (Independent of Device and Location)

mobile business

Benefits of Cloud Computing

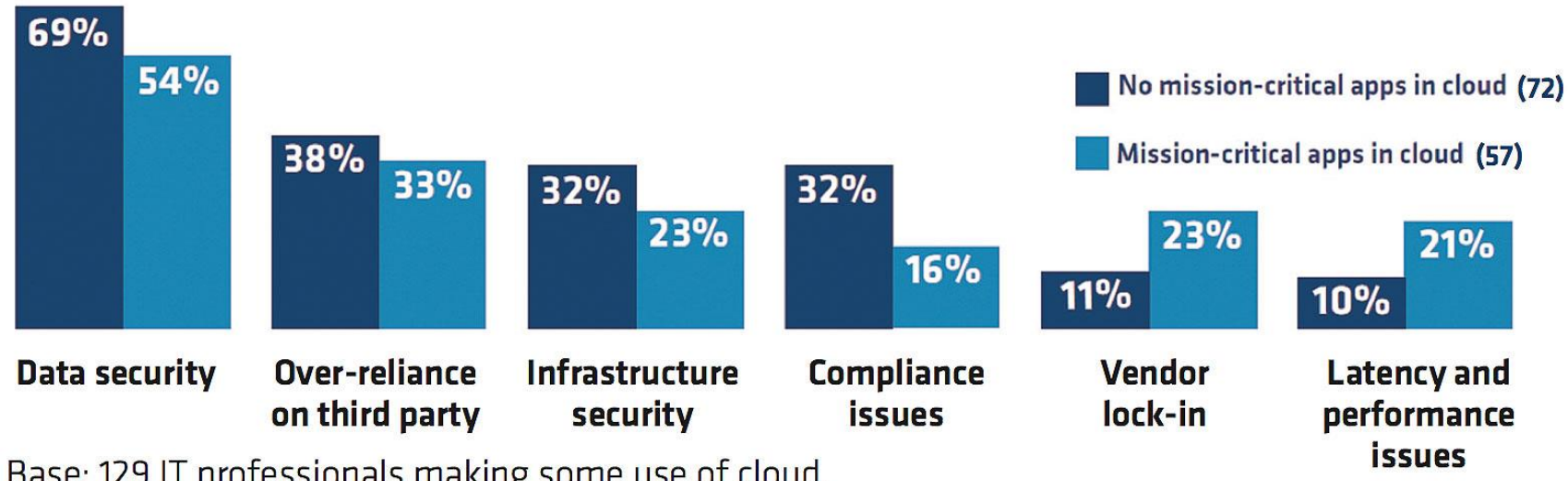


Why not using Cloud Computing?

- **Concerns of Cloud Computing**
  - Security
  - Complexity
  - Regulations and legal issues
  - Migration
  - Lack of standards
  - Limited customization
  - Costs
  - Issues of privacy

Concerns of Cloud Computing

2. What is preventing you making greater use of the cloud?



Base: 129 IT professionals making some use of cloud.

Security has been identified as one of the major concerns for widespread adoption of cloud computing.

[Source: computing.co.uk, 2012]

Compliance Issues

- Mostly concerns data storage
  - Location of storage
  - Processes for deleting data
  - Recovery plans / Business contingency

- To comply with regulations
  (e.g. the EU Data Protection Directive / Regulation)
  - users may have to adopt private, *community* or *hybrid* deployment modes
    ⇒ typically more expensive

Compliance Challenge: Resource Availability

- **Prolonged Outages**
  - FBI seized DigitalOne's thousands of servers for investigation in 2011
  - Especially SaaS-Provider close their business if it does not work out for them

Lock-In Effect

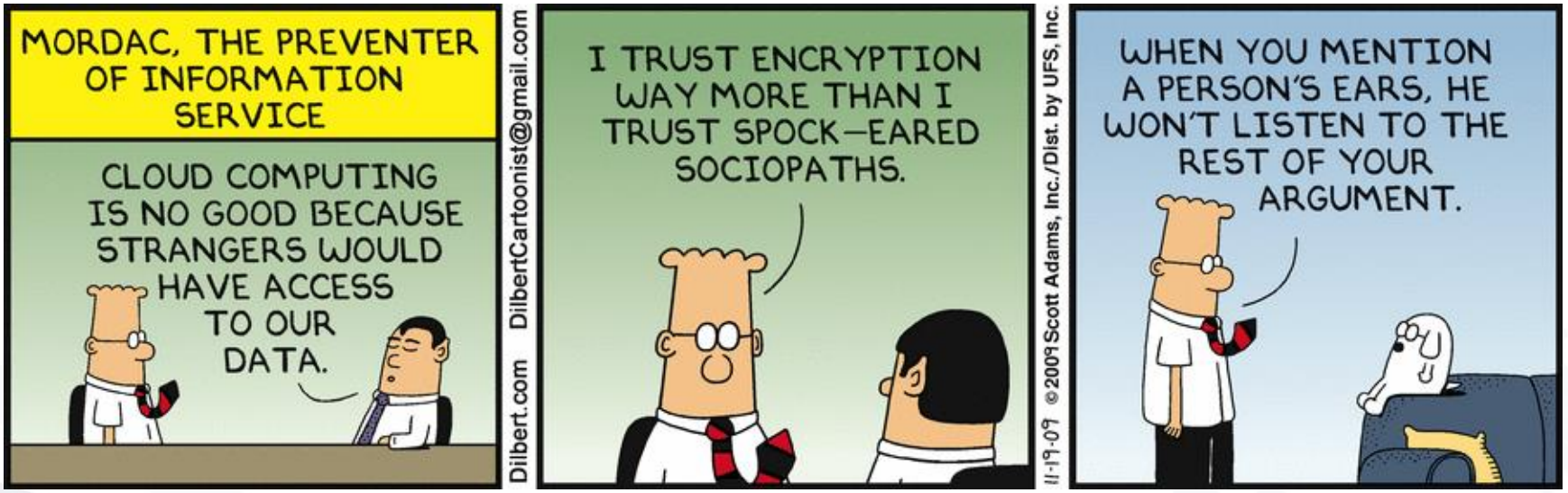
- Many cloud platforms are proprietary
- Lack of standards

⇒ tools and protocols
developed by/for particular vendor
⇒ migrating complicated + expensive

- Platform lock-in: e.g. VMWare vs Xen.
- Data lock-in: who actually owns the data?
- Tools lock-in: built tools may not be compatible

mobile business

Cloud Security



Traditional System Security vs Cloud Computing Security

Securing House
Owner and User are the same person

Users' biggest concerns

- Securing the perimeter
- Checking for intruders
- Securing the assets

Securing Apartment For Rent
Owner and User are not the same person

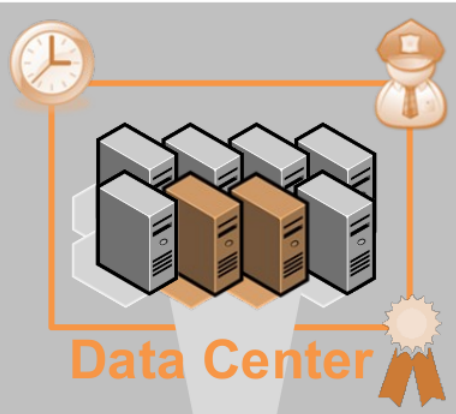
Users' biggest concerns

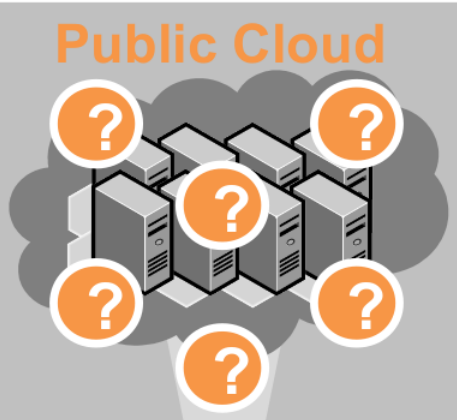
- Securing the apartment against the bad neighbor and/or the Owner

Security Concerns in Cloud Comp.

- Security is a major concern [Mell and Grance, 2009]
- Analysis of risks and threats [Cloud Security Alliance, 2010], [ENISA, 2009]
  ⇒ insider attacks and malicious insiders are a major technical risk
- Risk amplified due disappearance of physical boundaries [Hay et al., 2011], [Pieters, 2011]
- Variety of parties involved in a cloud service
  ⇒ cloud customers face difficulties in assessing risks and threats

Why is Cloud Security Perceived as Such a Big Problem?





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.

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?

- Loss of control, perceived or real
- Lack of experience
- No established standards
- Uncertainty on how to interpret regulations and practices

- Effects
  - Public clouds rarely used for mission critical workloads
  - Preference for application-as-a-service
  - Preference for private and hybrid cloud

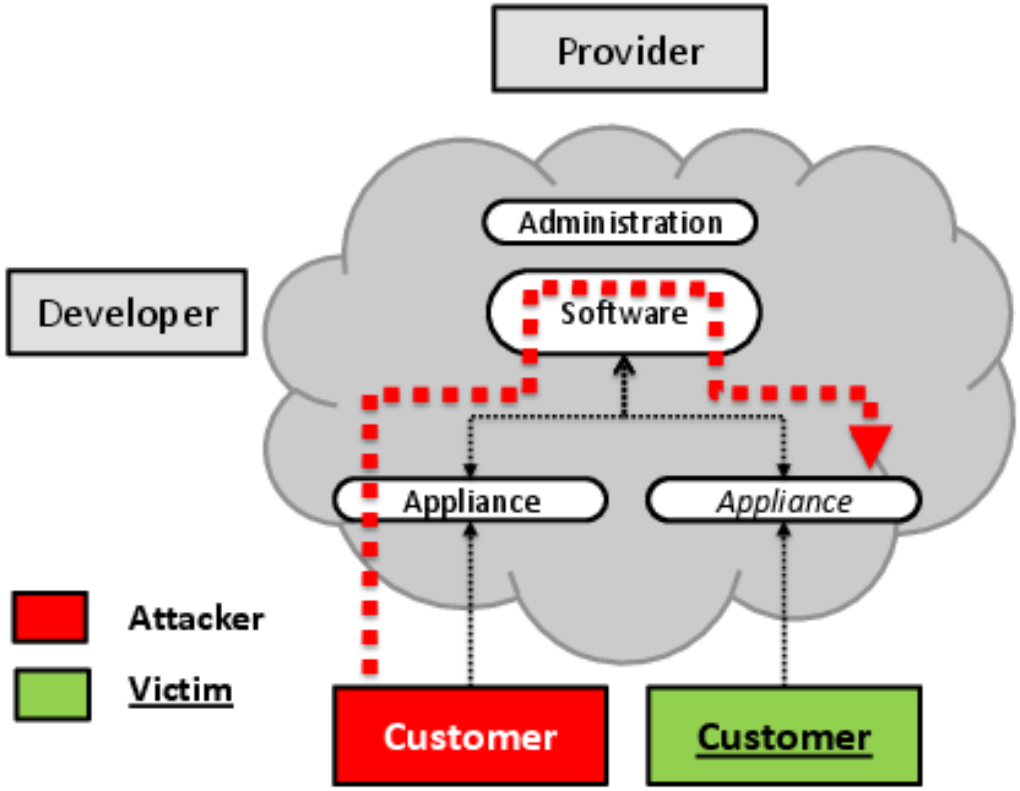
Sample Threats in Cloud Comp.

- Malicious administrator attacks VM [Rocha and Correia, 2011]
- Malicious customer attacks other customers who share physical resources [Ristenpart et al., 2009]
- Honest fault of a cloud administrator ⇒ outage of Amazon EC2 in 2011 [Amazon Web Services, 2011]
- Honest fault of cloud customers: [Bugiel et al., 2011]
  - SSH public key for admin account in image
  - private SSH keys, Amazon credentials in image

Security Challenge: Multitenancy

- **Problem**
  - Consumers **share applications/data** with other consumers that are unknown to them
  - Virtualization mechanisms are used to partition a physical resource into multiple virtual ones
  - Attacker or Malicious consumers can overcome virtualization mechanisms to gain unauthorized access

Virtual Machine Escape



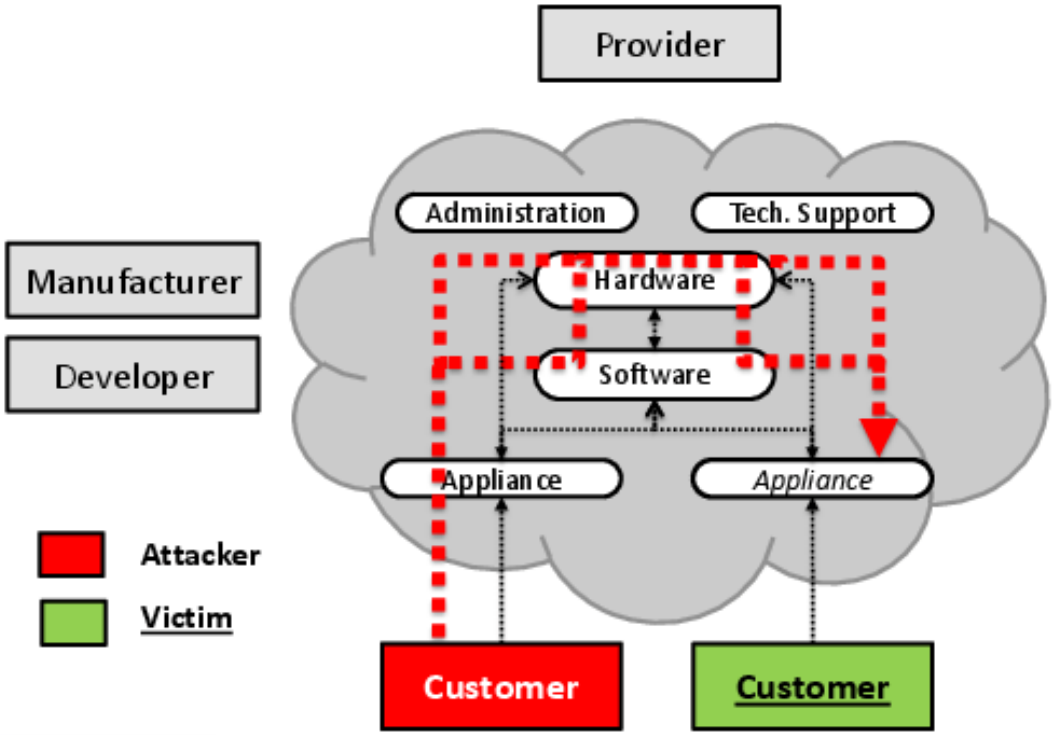
- Customer attacks other customers
- Provider should try to prevent this, but may not succeed
- Confidentiality, Integrity and Availability of service may be violated

Security Challenge: Multitenancy

- **Side-channel attack**
  - Attacker's virtual machine is able to extract sensitive information from the victim's virtual machine

[Source: Tromer]

Side-Channel Attacks



- Customer eavesdrops on other customers (e.g. to get crypto keys)
- Shared ressources always means there may be some way to observe others
- Confidentiality may be violated

Security Challenge: Loss of Control

- **Problem**
  - Data, applications, resources are located with cloud provider
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumers rely on provider to ensure data privacy and security

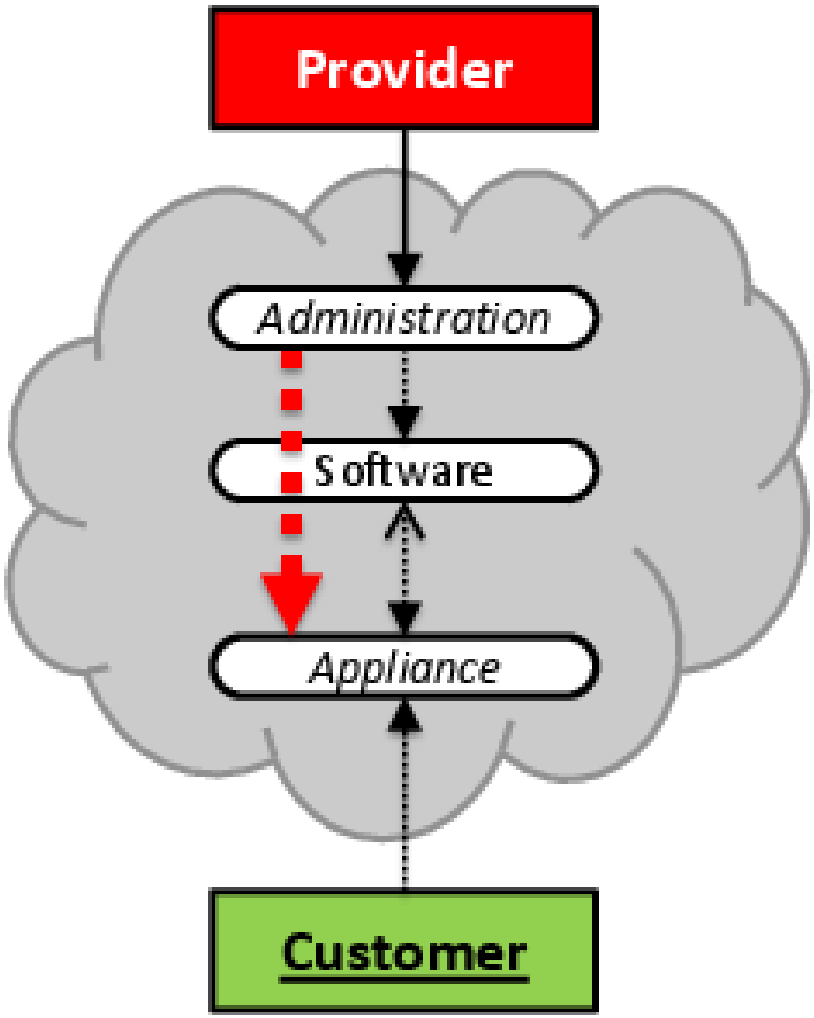
Security Challenge: Loss of Control

- **Data Breaches**
  - Dropbox experienced a data breach in 2011
  - For 4 hours users were able to login into accounts without any password
  - Possible to login into someone else account just typing his/her email address

Security Challenge: Insider Threats

- User needs to trust provider
  - But employee could be malicious insider who can easily obtain passwords, cryptographic keys, files and other confidential data.
- Countermeasures
  - Segregation of duties
  - Four eye principle
  - Background checks

Malicious Administrator



Attacker

Victim

- Provider may be malicious incompetent or just lazy
- Confidentiality, Availability and Integrity of service may be violated

Conclusions

- Cloud Computing is **flexible** and **cost-effective** to deliver computing resources
- **Security** is a **major barrier** to the **adoption** of Cloud Computing
- Main Security Challenges
  - **Multi-Tenancy**
    - Side-channel attacks
  - **Loss of Control**
    - Data Breaches, Data Loss, Insider Threats, Compliance, Privacy

Cloud Provider Selection

[Source: Cloudtweaks.com]

Cloud Service Provider Selection

Cloud Service Characteristics

- Tenant selects Provider
- Service Level Agreements
- Long-Term Relationship (Lock-In Effect)
- Tenant saves money?

- **Tenant transfers control and decisions**

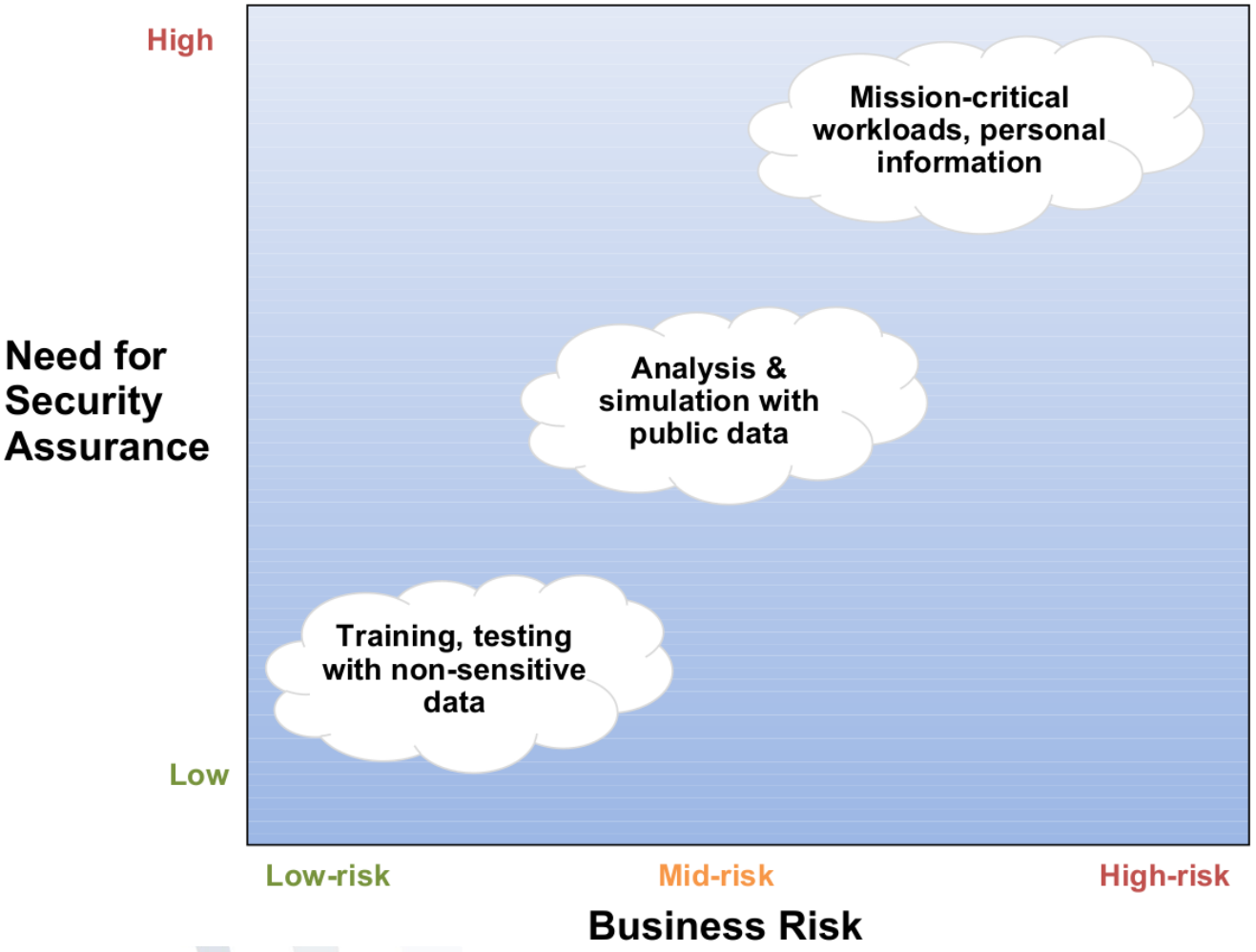
Challenges of CSP Selection

- Tension between tenant and provider

- Information asymmetry
  - Lemon Market [Akerlof, 1970]
  - Costs of Decision
  - Costs of Contract Negotiation [Tirole, 2009]
  - Costs of Controlling Provider

One size does not fit all

Different cloud workloads have different risk profiles



Tomorrow's high value / high risk workloads need:

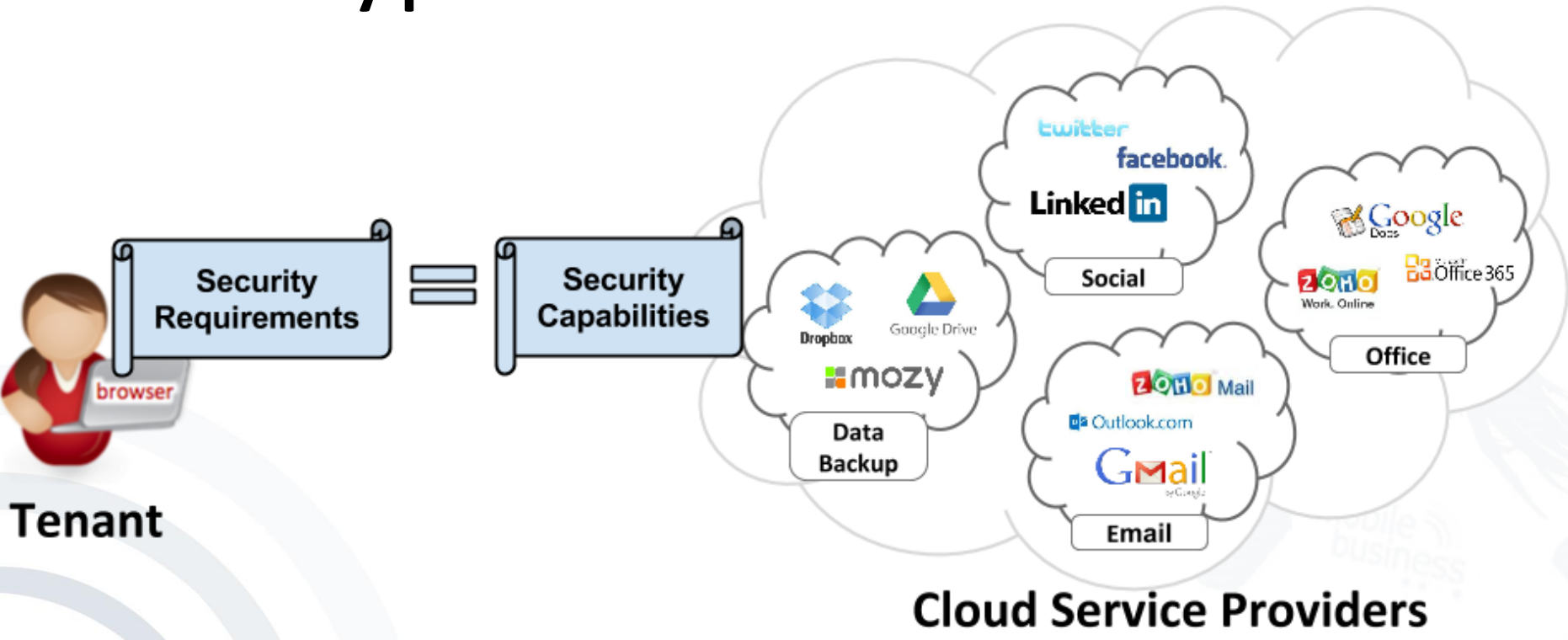
- Quality of protection adapted to risk
- Direct visibility and control
- Significant level of assurance

Today's clouds are primarily here:

- Lower risk workloads
- One-size-fits-all approach to data protection
- No significant assurance
- Price is key

Cloud Provider Selection

- **GOAL: Select a provider based on the level of security provided**



Security Requirements

Typical Security Requirements Derived from Privacy and Accountability Regulations

Legislation Area	Covers	Implications on Cloud Architecture
Corporate Financial Accounting and Reporting	Providing evidence of appropriate Business Controls, correct handling of financial data, correct reporting of financial information	**Extensive logging incl. provenance, demonstrable security controls between customers and between layers of the Cloud**
Financial transaction handling	Security measures necessary in order to service financial transactions and customers	Identification and segregation of the cloud elements supporting financial transactions **Data encryption**
Data Privacy	Security measures necessary in handling personal data	**Inability to move data around the cloud, data may have to reside and be processed within a specific country** Requirement on the cllient to manage data protection
Reserved Powers	Discovery, search and seizure powers retained as a matter of law by external agencies	**Data, audit logs, hardware may need to be discovered and surrendered to authorized agencies**
Restrictions on data transmittal and usage	Limitations or requirements to be fulfilled before data can be moved or used in different legislative domains	**Inability to move data around the cloud, data may have to reside and be processed within a specific country**
Industry-specific Regulatory issues	Requirements on specific industry sectors which will impact usage of Cloud	Industry-specific cloud implementations

Not a complete listing, not intended as legal advice.

Exercise

Excercise

- Try Cloud Service Provider Selection in Practise

- 1. aim: Get a feeling about the task
- 2. aim: Compare students from different subjects and locations

What we are going to do

- **This is an exercise to select a cloud service provider based on the level of security that it offers**
- **You will impersonate a tenant who has to choose a cloud provider based on your security requirements**
- **This is not an exam and you will not be evaluated based on this exercise**

mobile business

Cloud Security Alliance

- Non-profit organization to promote security best practices within cloud computing

- **Cloud Security Alliance Trust, Security and Assurance Registry (STAR)**
  - Publicly accessible registry listing the security controls provided by a cloud service provider
  - Tenants may use this information to select a cloud service provider

mobile business

Cloud Control Matrix

- **Cloud Control Matrix (CCM)**
  - **List of 295 security controls grouped in 16 categories**
- **Consensus Assessments Initiative Questionnaire (CAIQ)**
  - **Set of questions answered by a cloud service provider**
  - **Questions mapped to the security controls in the CCM**
  - **Answers should give an idea of the security of the provider**

Cloud Control Matrix II

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSIO

Control Domain	CCM V3.0 Control ID	Updated Control Specification	NERC CIP	NIST SP800-53 R3	NIST SP800-53 R4 App J	
Datacenter Security - Secure Area Authorization	DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	CIP-006-3c R1.2 - R1.3 - R1.4	PE-7 PE-16 PE-18		8.2 8.1
Datacenter Security Unauthorized Persons Entry	DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss		MA-1 MA-2 PE-16		8.1 8.2 8.3 8.4
Datacenter Security User Access	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.	CIP-006-3c R1.2 - R1.3 - R1.4 - R1.6 - R1.6.1 - R2 - R2.2	PE-2 PE-3 PE-6 PE-18		8.1 8.2
Encryption & Key Management	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies				

Consensus Assessments Initiative Questionnaire

Consensus Assessment Questions	Consensus Assessment Answers			Notes
	Yes	No	Not Applicable	
Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?				
Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?				

Selection vs. Comparison

Phase 1 (~30min)

1. **We give you a scenario description**
2. **Identify security requirements for the given scenario**
3. **We provide you a list of categories for security requirements**
4. **Map the security requirements to the security categories**
5. **Depending on the importance of each category give each category a score from 1 (low important) to 9 (very important) with no more than 100 in total.**

Phase 2 - 4

- **Phase 2 (5min)**
  - **Answer a questionnaire to reflect your last task https://www.isurvey.soton.ac.uk/20082**
- **Phase 3 (40min)**
  - **You will get CAIQs from two providers. Given the scenario description and your previously created scores, judge which of the providers may be the best for the scenario**
- **Phase 4 (10min)**
  - **Answer a questionnaire to reflect your last task https://www.isurvey.soton.ac.uk/20082**