Security and Privacy in Cloud Computing ENISA perspective

Giles Hogben

European Network and Information Security Agency

What's new about Cloud Computing?

Isn't it just old hat?

Larry Ellison, CEO, Oracle

"The computer industry is the only industry that is more fashion-driven than women's fashion."

"I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads."

Presentation Overview

- ENISA perspective and work
  - SME migration
  - eGovernment/eHealth
  - Resilience
- **Good News: Security Benefits** of Cloud Computing
- **Bad News: Security Risks** of Cloud Computing
- Recommendations (work in progress)

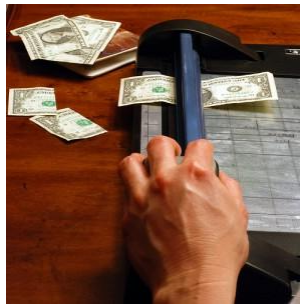
What is Cloud Computing?

Cloud computing is an on-demand service model for IT provision **usually** based on virtualization and distributed computing technologies:

- Highly **abstracted** resources
- Near **instant scalability** and flexibility
- Near **instantaneous provisioning**.

What is Cloud Computing?

- **Shared resources** (hardware, database,memory, etc...)
- '**Service On demand**', usually with a '**pay as you go**' billing system
- **Programmatic management** (e.g. through WS API)



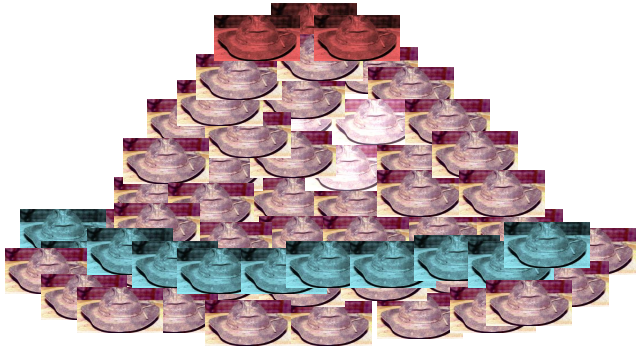
Source Flickr user ysella

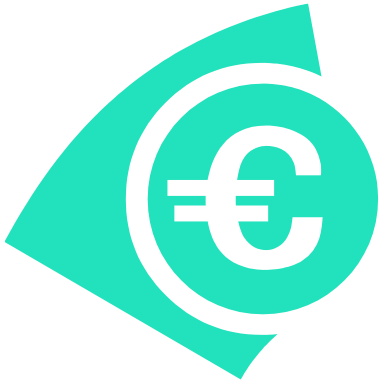
enisa
European Network and Information Security Agency

Yes it is OLD HAT!

LOTS AND LOTS of old hat, put together with some very clever resource distribution algorithms

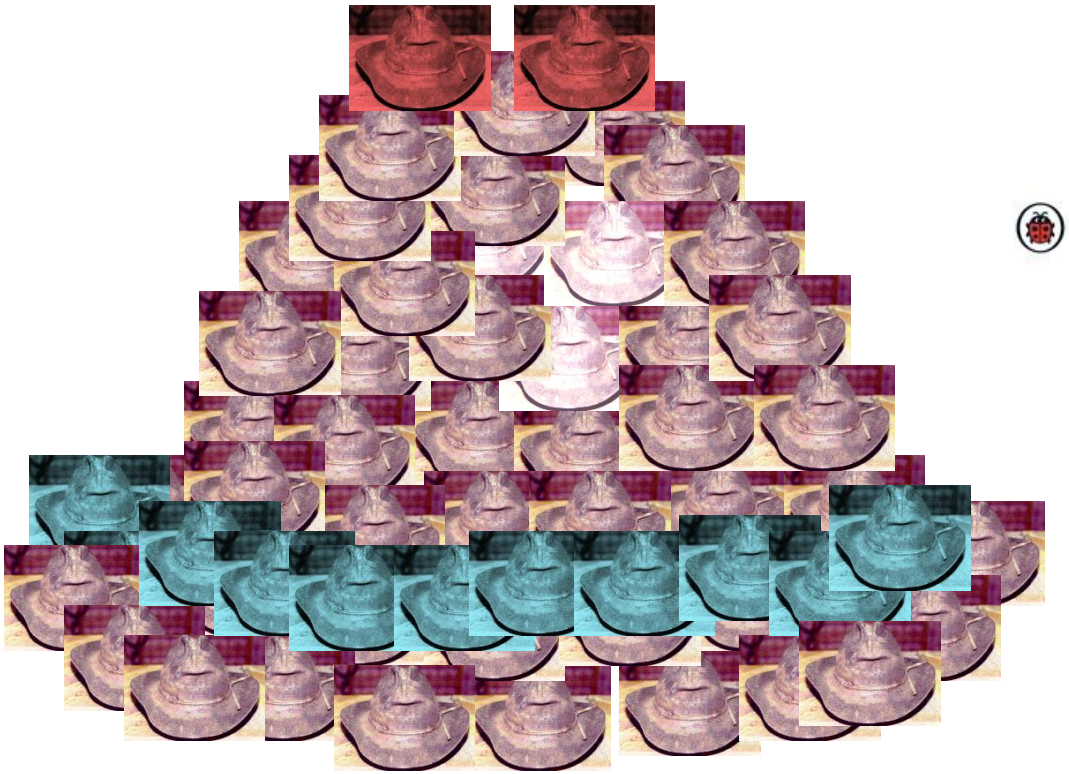
To make NEW Hat





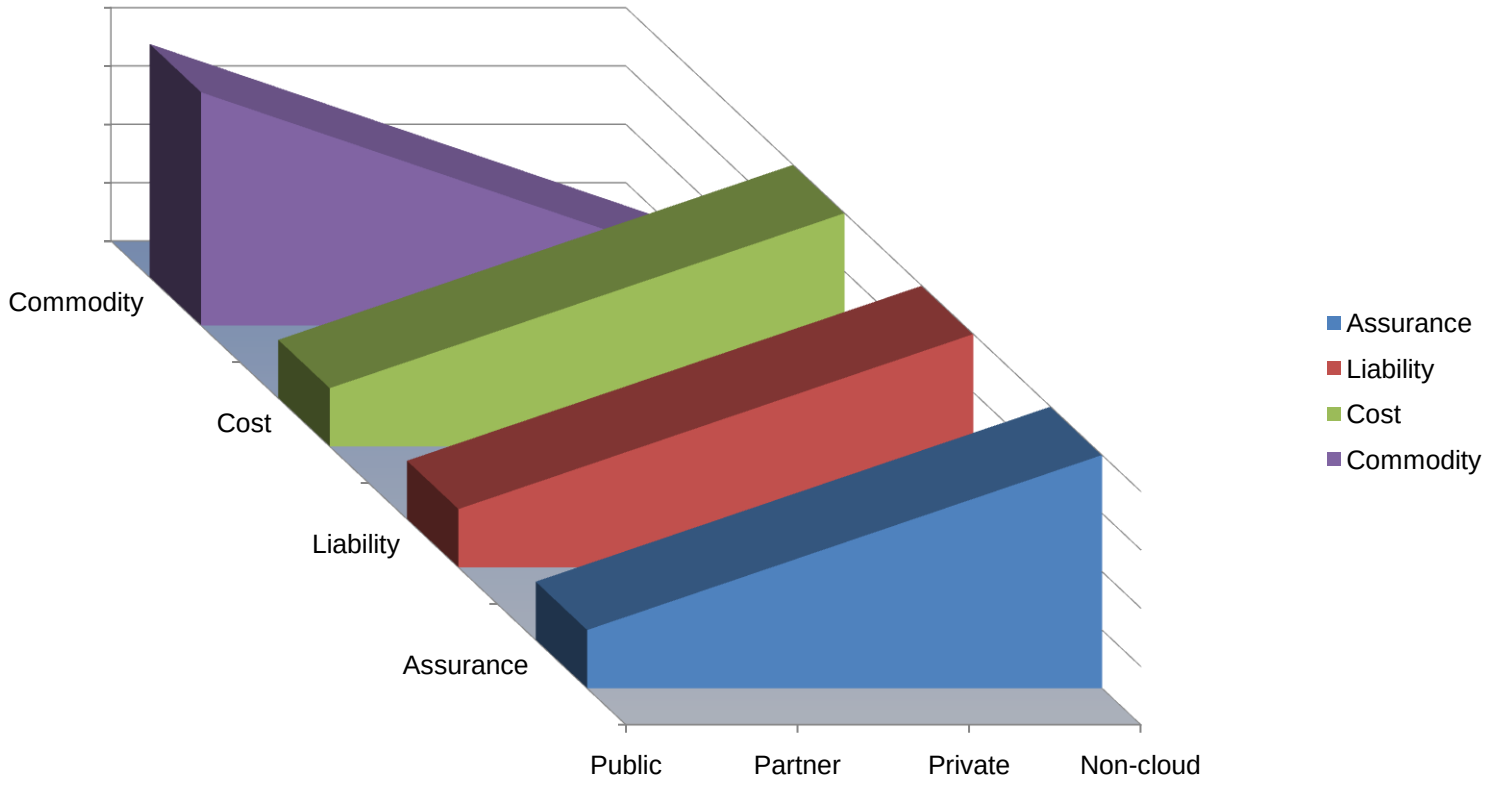
Which you can rent by the hour

MR. CHATTERBOX
By Roger Hargreaves



And – the more you talk, the bigger it gets (and vice-versa)

Types of cloud



ENISA Risk Assessment of Cloud Computing Technologies

- Scenario description - selected scenarios:
  - **SME Migration**
  - **Resilience**
  - **Government eHealth**
- Analysis of risks (Assets, Vulnerabilities, Threats)
- **Recommendations**
- Using ENISA Emerging and Future Risk Framework

Our Expert Group

- Amazon
- Avenade
- BT
- Bologna University
- Cisco Systems
- Cloudsecurity.org (Craig Balding)
- Ebay
- Fujitsu Labs Europe
- Spire Security
- Google
- HP
- IBM
- Microsoft
- Reservoir Project
- Symantec
- Cloudsecurity.org (Craig Balding)
- The Israeli Association of GRID Technologies (IGT)
- UCL
- Virtualisation.info

+ Liason with CSA (Cloud Security Alliance)

Example Scenarios

SME Scenario: Security risks for an SME migrating to the cloud.

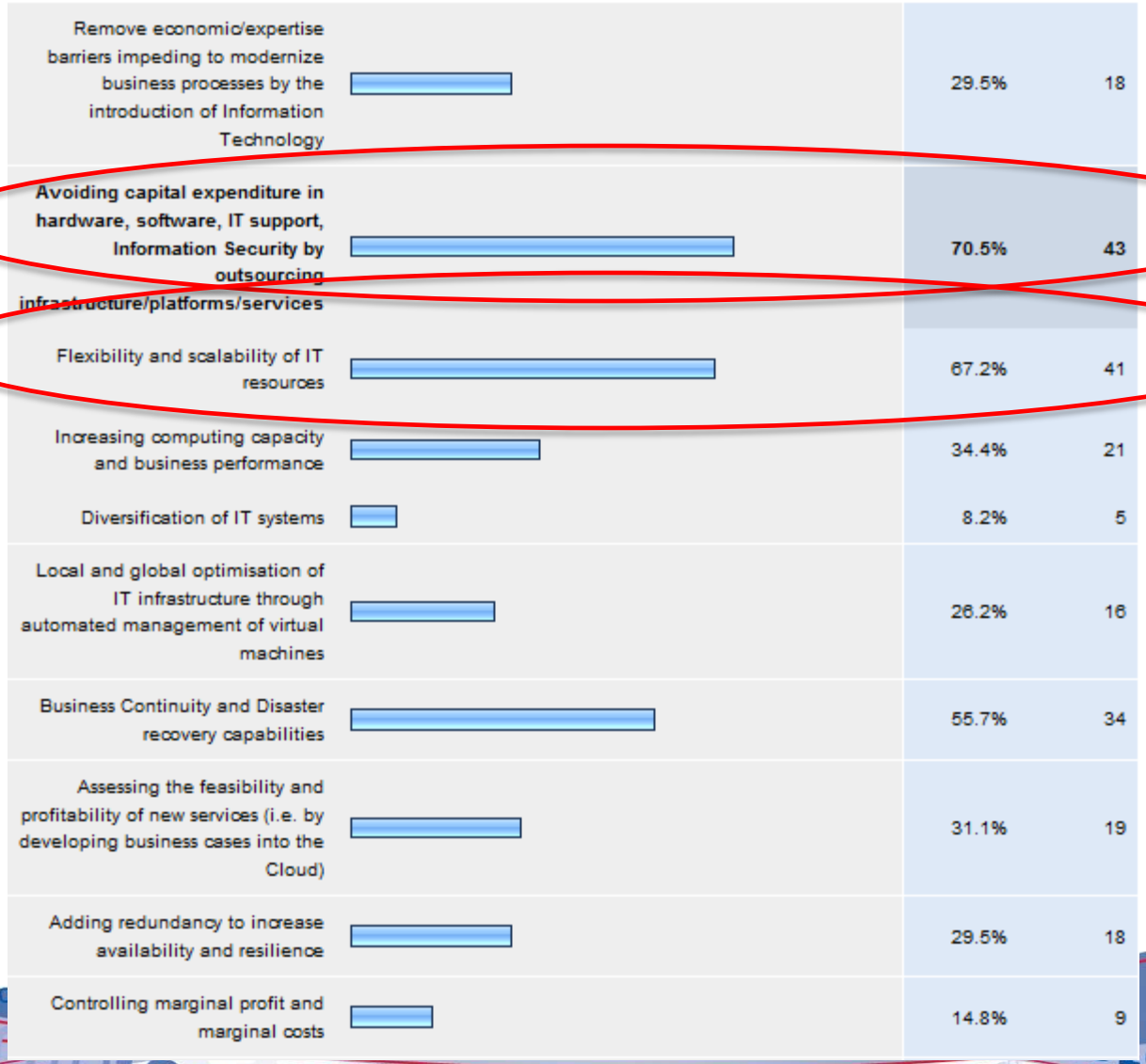
Name: Clean Future

Business Sector: Solar panels.

Based in: Germany with 3 branch offices in Europe

Employees: 93 people and between 10 and 30 contractors (interim agents, sales representatives, consultants, trainees, etc.).

SME's - Reasons for adoption



Remove economic/expertise barriers impeding to modernize business processes by the introduction of Information Technology	29.5%	18
Avoiding capital expenditure in hardware, software, IT support, Information Security by outsourcing infrastructure/platforms/services	**70.5%**	**43**
Flexibility and scalability of IT resources	67.2%	41
Increasing computing capacity and business performance	34.4%	21
Diversification of IT systems	8.2%	5
Local and global optimisation of IT infrastructure through automated management of virtual machines	26.2%	16
Business Continuity and Disaster recovery capabilities	55.7%	34
Assessing the feasibility and profitability of new services (i.e. by developing business cases into the Cloud)	31.1%	19
Adding redundancy to increase availability and resilience	29.5%	18
Controlling marginal profit and marginal costs	14.8%	9

SME's: Main Concerns

	Not Important	Medium Importance	Very Important	Showstopper	Rating Average	Response Count
Privacy	0.0% (0)	12.3% (7)	**43.9% (25)**	**43.9% (25)**	3.32	57
Availability of services and/or data	1.8% (1)	10.9% (6)	**47.3% (26)**	40.0% (22)	3.25	55
Integrity of services and/or data	0.0% (0)	13.0% (7)	42.6% (23)	**44.4% (24)**	3.31	54
Confidentiality of corporate data	1.8% (1)	3.6% (2)	30.9% (17)	**63.6% (35)**	3.56	55
Repudiation	2.1% (1)	41.7% (20)	**47.9% (23)**	8.3% (4)	2.63	48
Loss of control of services and/or data	3.8% (2)	20.8% (11)	**47.2% (25)**	28.3% (15)	3.00	53
Lack of liability of providers in case of security incidents	2.0% (1)	25.5% (13)	**43.1% (22)**	29.4% (15)	3.00	51
Inconsistency between trans national laws and regulations	11.8% (6)	**43.1% (22)**	23.5% (12)	21.6% (11)	2.55	51
Unclear scheme in the pay per use approach	14.0% (7)	**46.0% (23)**	24.0% (12)	16.0% (8)	2.42	50
Uncontrolled variable cost	4.1% (2)	36.7% (18)	**46.9% (23)**	12.2% (6)	2.67	49
Cost and difficulty of migration to the cloud (legacy software etc...)	14.3% (7)	**53.1% (26)**	22.4% (11)	10.2% (5)	2.29	49
Intra-clouds (vendor lock-in) migration	8.3% (4)	**37.5% (18)**	35.4% (17)	18.8% (9)	2.65	48

IT and Security requirements

- Managed security services
- Business Continuity and Disaster Recovery
- A test-bed for assessing new applications
  - Business efficiency and innovation capacity

Resilience Scenario

Resilience:

"The ability of a system to provide & maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation."

Resilience Scenario

- Service requiring high
  - availability, reliability, integrity and confidentiality
- Focus on resilience of cloud computing against
  - DDoS
  - Natural Disaster
  - Misuse of platform

XK-Fin

- Real-time price data and charts for goods in purchasing portals
- Historical data for use in price-prediction and analysis
- Order histories and stock control reports for companies.
- Real-time currency conversion and FX histories

Scenario characteristics – comparing resilience:

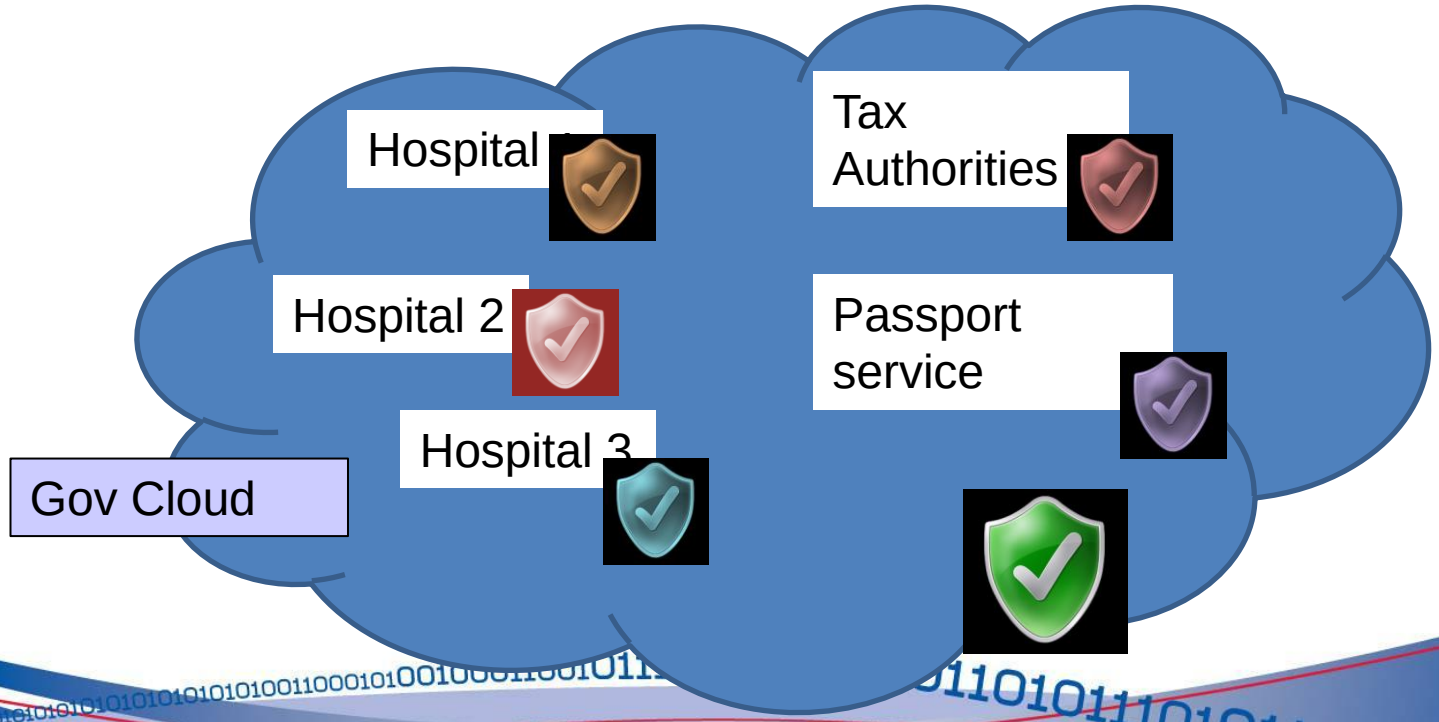
- 2007 – traditional infrastructure
  - Typical data centre managed by XK
  - Multi-homed
  - SAN off-site backup
  - No SLA

- 2012 –cloud infrastructure
  - Shared resources (including network, filtering etc...) with smart management algorithms.
  - Faster and cheaper scaling of resources
  - SLA of XK and cloud provider
  - Cloud disaster recovery

eHealth/government Scenario

★ eHealth services running on a PRIVATE GOVERNMENT CLOUD

Security Policy



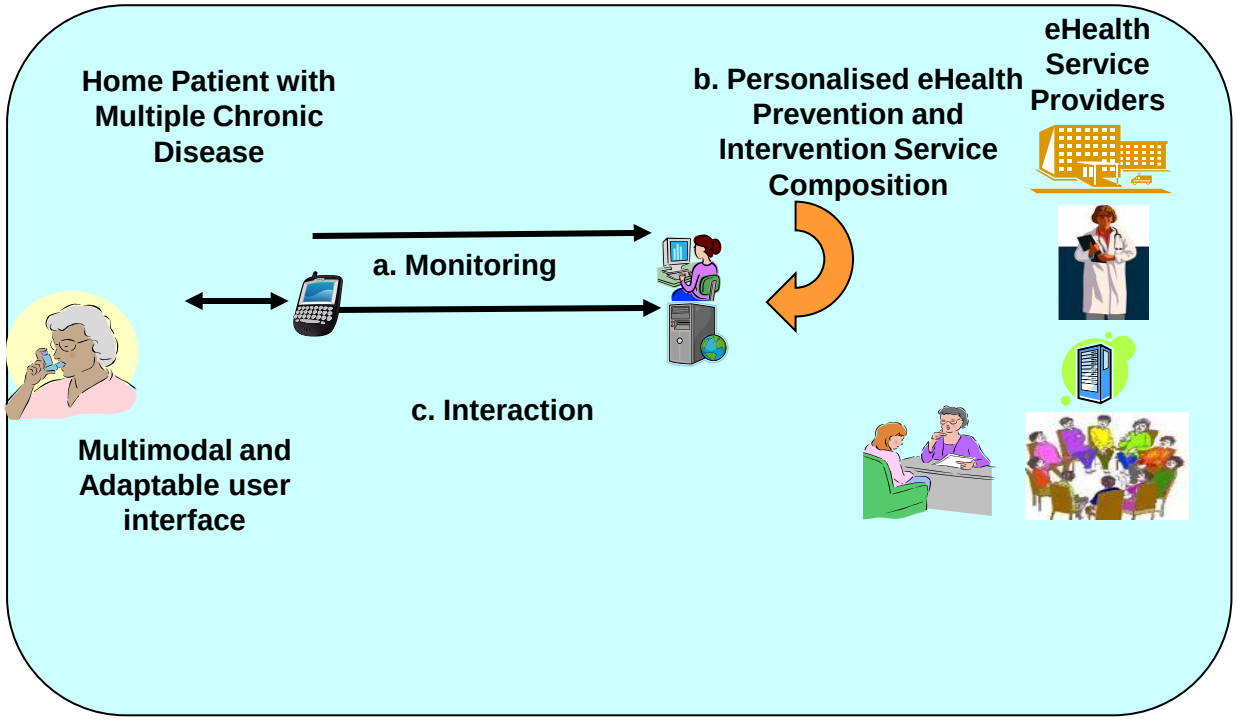
Gov-cloud

- Several different government departments share the same computing infrastructure.
- The cloud is built by a third party provider but is owned and controlled by the government.
- The cloud provides a (high) baseline security policy
- Individual departments can add controls.

Scenario – remote monitoring using Gov-Cloud

- Home devices monitoring patients use Gov-Cloud to store data.
- The services running at the monitoring center are running on the cloud using IaaS.
- Monitored data is also stored in the cloud using Database as a Service (DaaS).
- The various eHealth service providers are using cloud computing infrastructures.

eHealth Scenario



Baseline security policy

- Data (including sensitive personal information) must be encrypted in transit and at rest (e.g. on mobile devices).
- Data processing must satisfy European data protection law – e.g. definition of ‘data processor’ for all operations.

Baseline Security Policy

- Data should not leave the original country of collection at any time.
- Integrity and availability are “guaranteed” in some instances.
- Sensitive data should be destroyed at a specified time in its lifecycle.

Baseline Security Policy

- Physical security controls of data centres assured e.g. by ISO 27001 certification.
- Senior staff are given special responsibility for the confidentiality of ‘patient and service-user information’.
- Any cloud computing service providers must ensure the right of audit of their policies, processes, systems and services.

Key problems:

- Individual government departments do not like the perceived loss of control over their security and infrastructure.
- Separation of roles.
- How to guarantee that data does not leave the jurisdiction.
- ISO controls are not adapted for clouds.

Security Benefits

enisa
European Network and Information Security Agency

www.enisa.europa.eu

Something positive

- **Security and economies of scale:** security measures are cheaper when implemented at larger scale.
  - E.g. Filtering, patch management, hardening of VM instances and hypervisors, human resources, vetting, hardware redundancy, strong authentication, efficient RBAC, federated identity management..

It’s not all bad news for security

- **Staff specialisation and experience**:
  - More mature incident response capabilities.
  - Cloud providers big enough to hire specialists in dealing with specific security threats.

It’s not all bad news for security

- **Other benefits of scale:**
  - **Multiple locations** by default -> redundancy and failure independence.
  - **Edge networks:** Storage, processing and delivery closer to the network edge.
  - **Security services can be commoditised**
  - **More competition:** open market in security service provision.

It’s not all bad news for security

- **Rapid, smart scaling of resources:**
  - e.g. storage, memory, VM images, bandwidth?, processing power (using smart queuing services) – good against DDoS
- **Including defensive resources:**
  - packet filtering, anomaly detection, traffic shaping and encryption/decryption resources.

It’s not all bad news for security

- Forensics and audit
  - Dedicated, pay-per-use forensic images of VMs
  - More cost-effective log storage
  - Pay-as-you-go = cheaper audit storage costs.

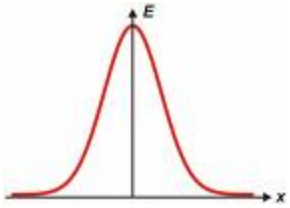
enisa
European Network and Information Security Agency

The Risks

Based on analysis of our 3 scenarios

A **RISK** is the consequence of a **THREAT** that exploited a **VULNERABILITY** that exists on an **ASSET**

- Threats have a certain level of impact 

and occur with a certain level of probability 

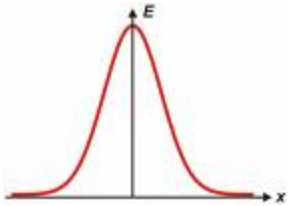
Informally

- What bad stuff could happen? **(Threat)**

- What or who could it happen to. **(Assets)**

- How is this possible? **(Vulnerabilities)**

- How likely is it? **(Probability)**



- Why worry? **(Impact)**

Very high value assets

- More Data in transit (Without encryption?)
- Federated IdM/Authentication (can take down multiple systems)
- Management interfaces – big juicy targets:

Very high value assets

- Trustworthiness of insiders.
- Hypervisors- hypervisor layer attacks on virtual machines are very attractive.
  - No known compromise without access to the hypervisor at this time.
  - BUT – any attacks on hypervisor (even internally) are extremely high impact.
  - (See http://invisiblethingslab.com/bh08/part3.pdf)

enisa
European Network and Information Security Agency

Top Risks

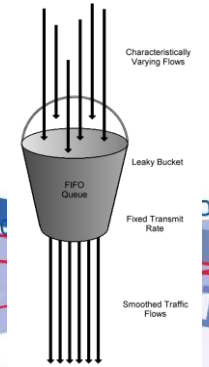
RESOURCE EXHAUSTION

★ Overbooking

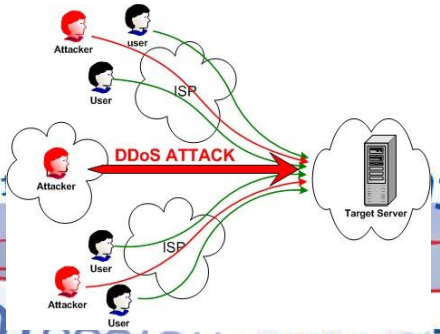
Underbooking

Caused by:

Resource allocation algos



Denial of Service



Freak events

Isolation failure

- Storage (e.g. Side channel attacks) see http://bit.ly/12h5Yh
- Memory
- Virtual machines
- Entropy pools (http://bit.ly/41sIiN)
- Resource use (e.g. Bandwidth)

Isolation failure- reputation

- Reputation can spread in unexpected ways
  - E.g. Blacklisting of subnet, outages.

Paediatrician attacks 'ignorant' vandals

The front door was daubed with yellow paint

A hospital paediatrician has hit out at vandals who forced her to flee her home after apparently taking her job title to mean she was a paedophile.

South African-born Yvette Cloete - a 30-year-old trainee consultant at the Royal Gwent Hospital, Newport, south Wales - said she planned to move home after returning to find the outside of her property daubed with the words "paedo".

She said she can not rule out the possibility that the paint attack was connected with her

Key management 1

- Key storage and provisioning almost impossible to do on-cloud with current technologies
  - HSM's don't scale to the cloud
  - PKCS#10,11 don't talk cloud
  - Revocation is even more complicated...
- Need new crypto and key management standards and solutions adapted to cloud paradigm.

Key management

- Key management is (currently) the responsibility of the cloud customer.
- Key provisioning and storage is usually off-cloud
- One key per account – doesn't scale to multiple accounts/account holders.

Photo: Alexander Klink

Identity provisioning and deprovisioning

- Multiple cloud providers
  - synching with the enterprise directory is not scalable.
  - Connection to enterprise leaves a single point of failure.
  - De-provisioning of identities is even less scalable since time lags are a window of opportunity for attackers.

A driver for Federated Identity

- FIM is the only solution which scales to the cloud.
- FIM applications themselves (except key storage) can be run using cloud infrastructure.
- Cloud-based IdP gives more resilience of overall system.

Data security

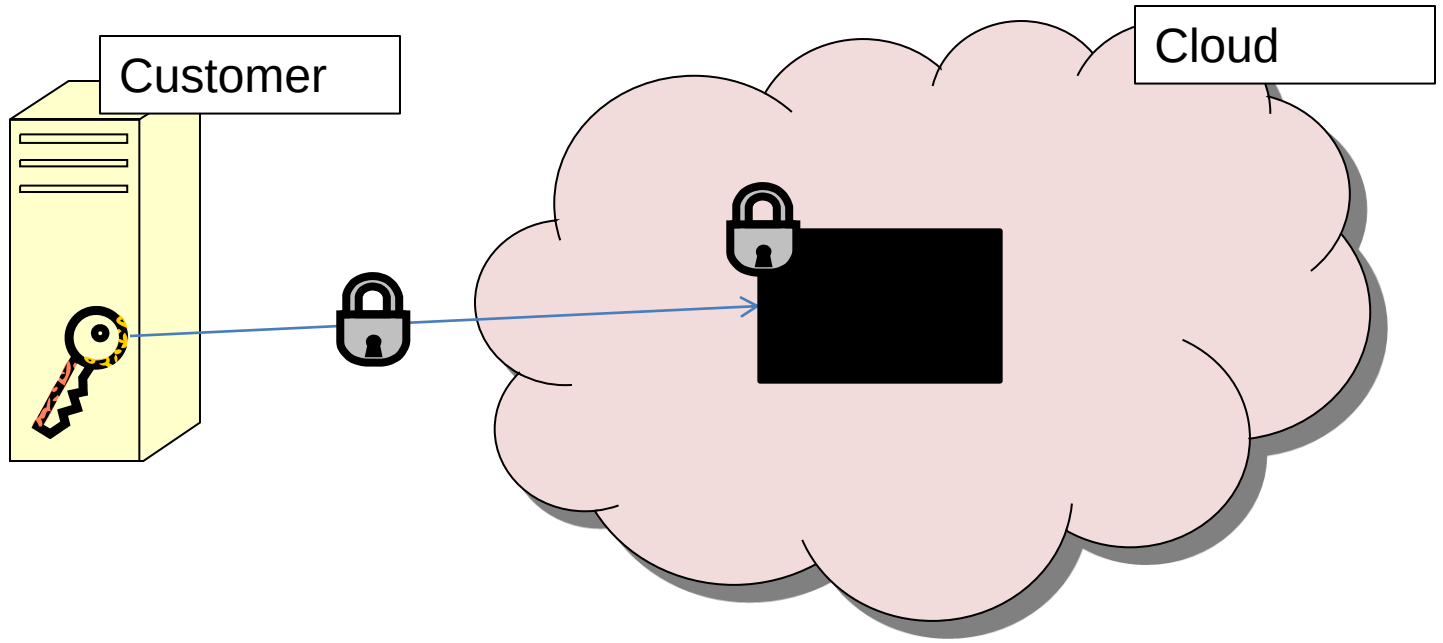
- External pen testing not permitted (Public clouds).
- External audit not permitted.
- Very limited logs available.
- Usually no forensics offered (ghosting a ghost – Craig Balding).
- No idea of actual location/jurisdiction of data.

Data security

- Encrypting data on-cloud so that the cloud provider can't read it is (very) hard!

Encryption: Data storage and processing without security guarantees?

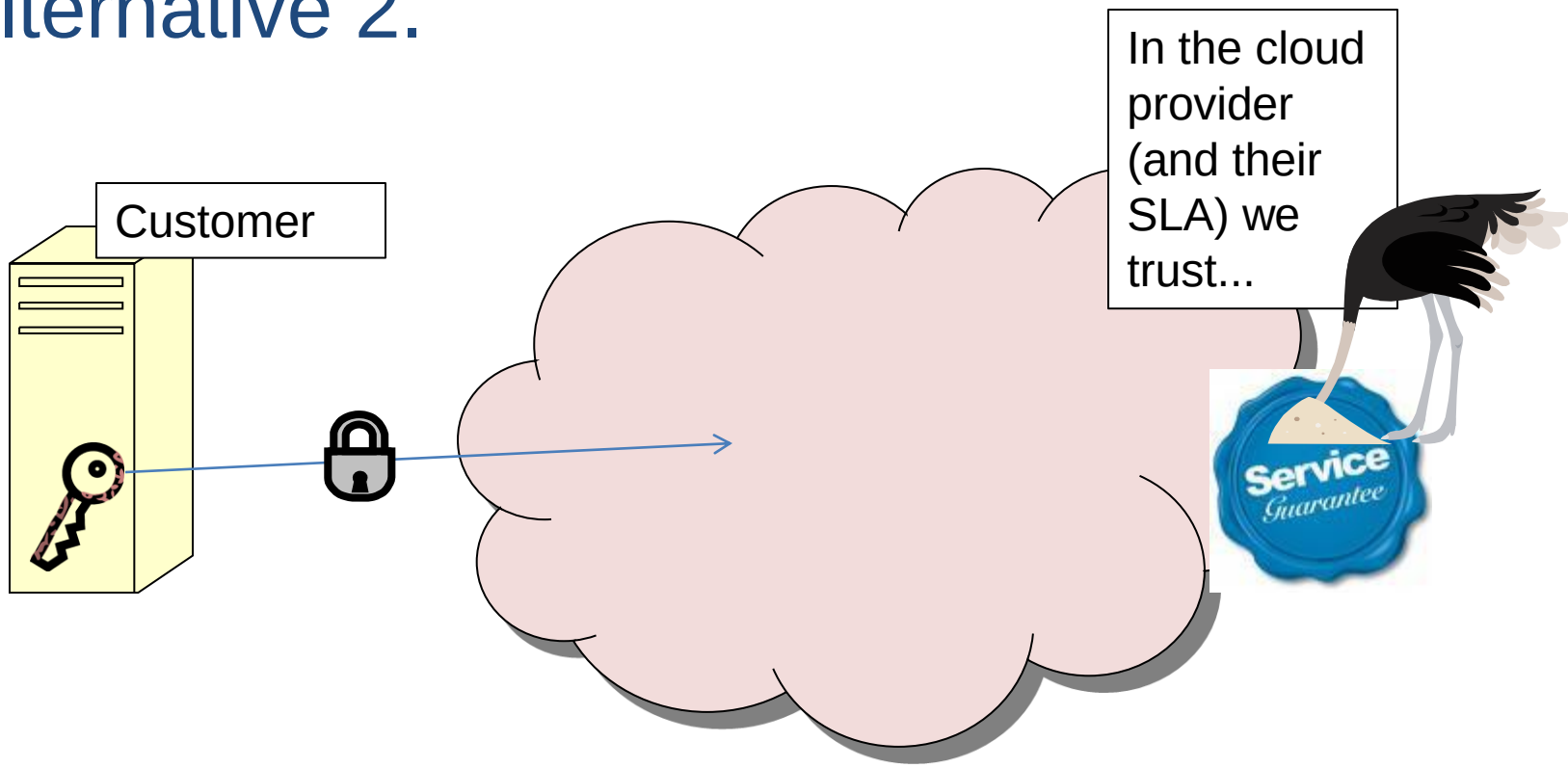
- Alternative 1. – HARD TO IMPLEMENT!



Try to encrypt all operations to hide them from the untrusted hardware

Data storage and processing without security guarantees?

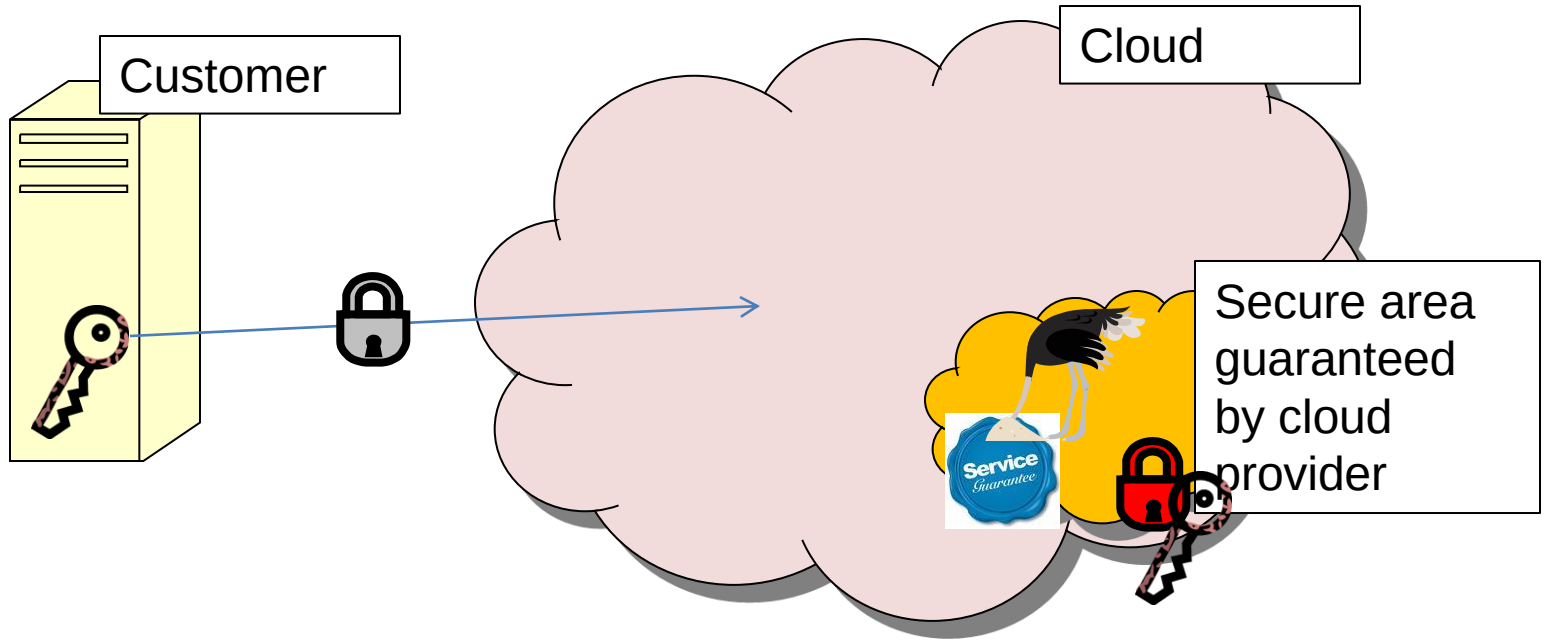
- Alternative 2.



Trust the cloud provider

Data storage and processing without security guarantees?

- Alternative 3.



Use a secure area with security guarantees provided by cloud provider

Other data protection issues

- Jurisdiction hell (E.g. UK NHS has a requirement that data does not LEAVE the UK)
- Hunt the data controller.
- Data deletion – destruction at end of lifecycle
- Sub-poena/legal suits

Assurance Overload

Assurance Overload

ISO 27001

"Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements."

Somebody else's problem (SEP) syndrome

"*Appirio Cloud Storage fully encrypts each piece of data as it passes from your computer to the Amazon S3 store. Once there, it is protected by the same strong security mechanisms that protect thousands of customers using Amazon's services* " (Thanks to Craig Balding, cloudsecurity.org for spotting this)

Amazon AWS ToS

- "YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA."

- "*You are personally responsible for all Applications running on and traffic originating from the instances you initiate within Amazon EC2. As such, you should protect your authentication keys and security credentials. Actions taken using your credentials shall be deemed to be actions taken by you.*"

Recommendations (work in progress)

- Certification Check-List (also to reduce audit burden)
  - E.g. Proper isolation measures.
  - Compatibility with federated identity systems
  - Multiple redundant sites
  - Employee vetting
  - Separation of roles and responsibilities.
  - Etc..

Research recommendations

- Maintaining state in live VM's
- Key management
- Load management and resource distribution
- Encrypted processing.

Government recommendations

- Public clouds are (usually) not suitable for government applications.
- Clearly define international differences in DP legislation.
- Should there be breach notification requirements on cloud providers.

Roles and Responsibilities

- Check your obligations wrt security
  - Do not assume your cloud provider encrypts your data.
  - Patching
  - Forensics

Contracts

- Check contract clauses
  - Intellectual property
  - Cloud provider failure/ get-out clauses.
  - Check outsourcing provisions.
  - Liability for data protection incidents.
- Application code portability: are there alternative providers that could host any custom application code you develop?

The Penultimate Slide

- Watch out for the results of ENISA's cloud security study – out in mid November (http://www.enisa.europa.eu)