

# CLOUD SECURITY

OR: HOW I LEARNED TO STOP WORRYING AND LOVE THE CLOUD

**Jakob I. Pagter  
(Alon Hazay)**

***Alexandra Instituttet A/S***

# About the Alexandra Institute

- Non-profit application oriented research institution – focus on IT
- GTS – Godkendt Teknologisk Service Institut
- 100+ employees

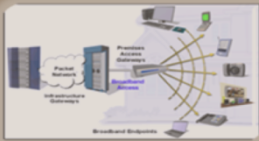


# Essential Characteristics of Cloud Computing



## On-demand self-service

- provision computing capabilities automatically without requiring human interaction



## Broad network access

- Capabilities are available over the network promote use by heterogeneous thin or thick client



## Measured Service

Resource usage can be monitored, controlled, and reported, providing transparency



## Rapid elasticity

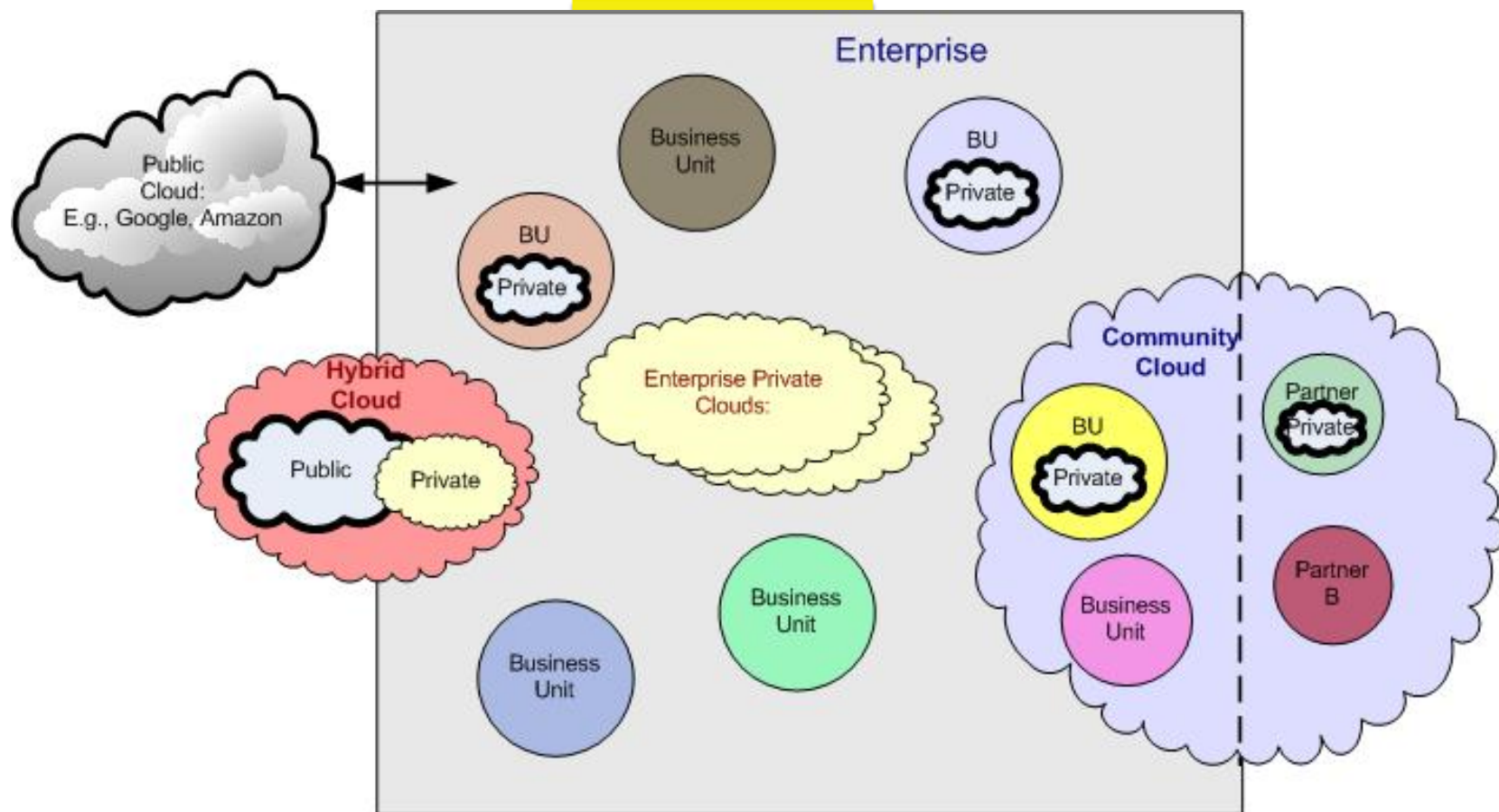
- Capabilities can be rapidly and elastically provisioned, automatically, to quickly scale out or rapidly scale in



## Resource pooling

- A sense of location independence. customer has no control or knowledge over the location of the resources

# Deployment Model



# Cloud Service Models -

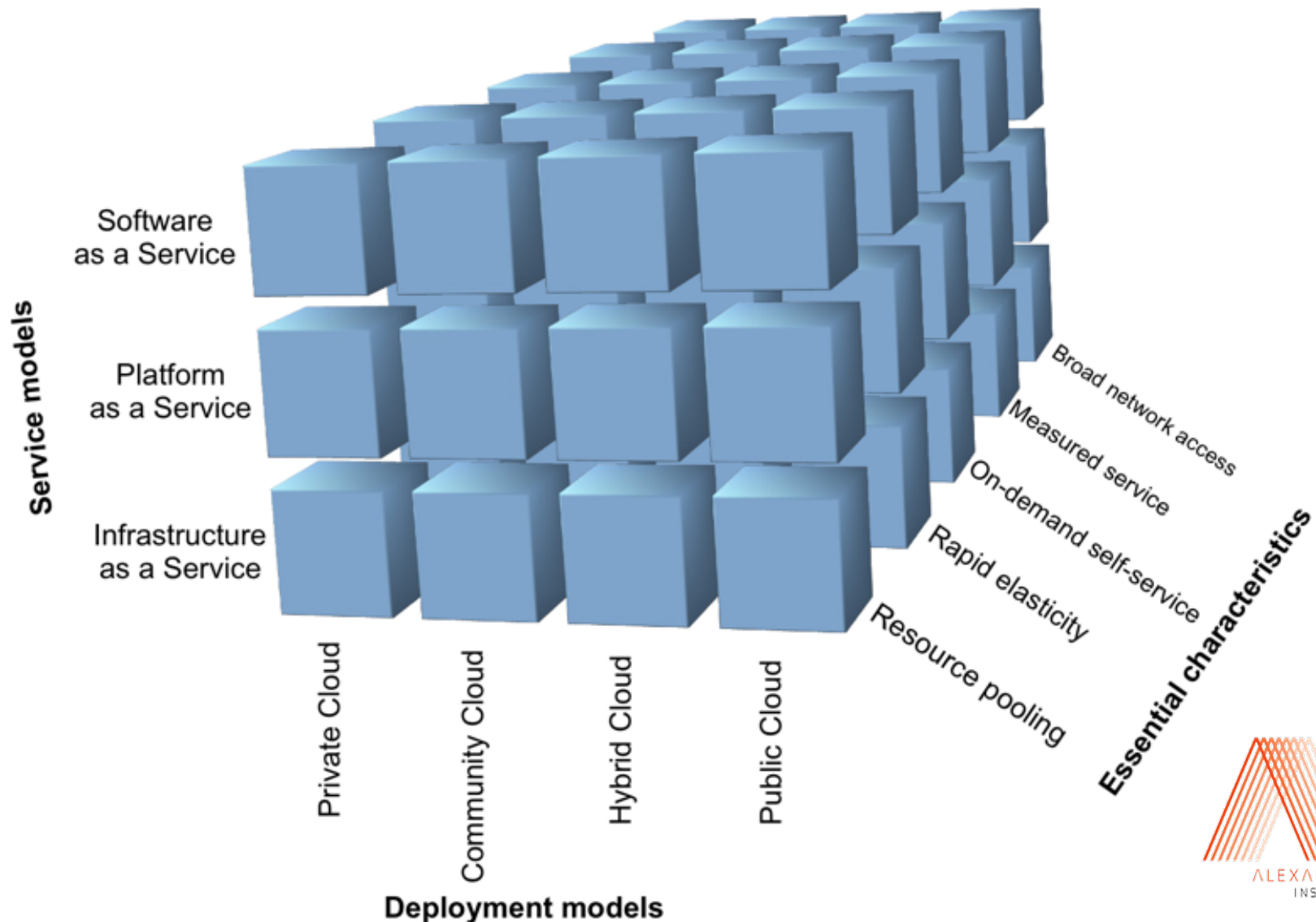
## Service Layers Definition



**Notes:**  
Brand names for illustrative / example purposes only,  
and examples are not exhaustive.

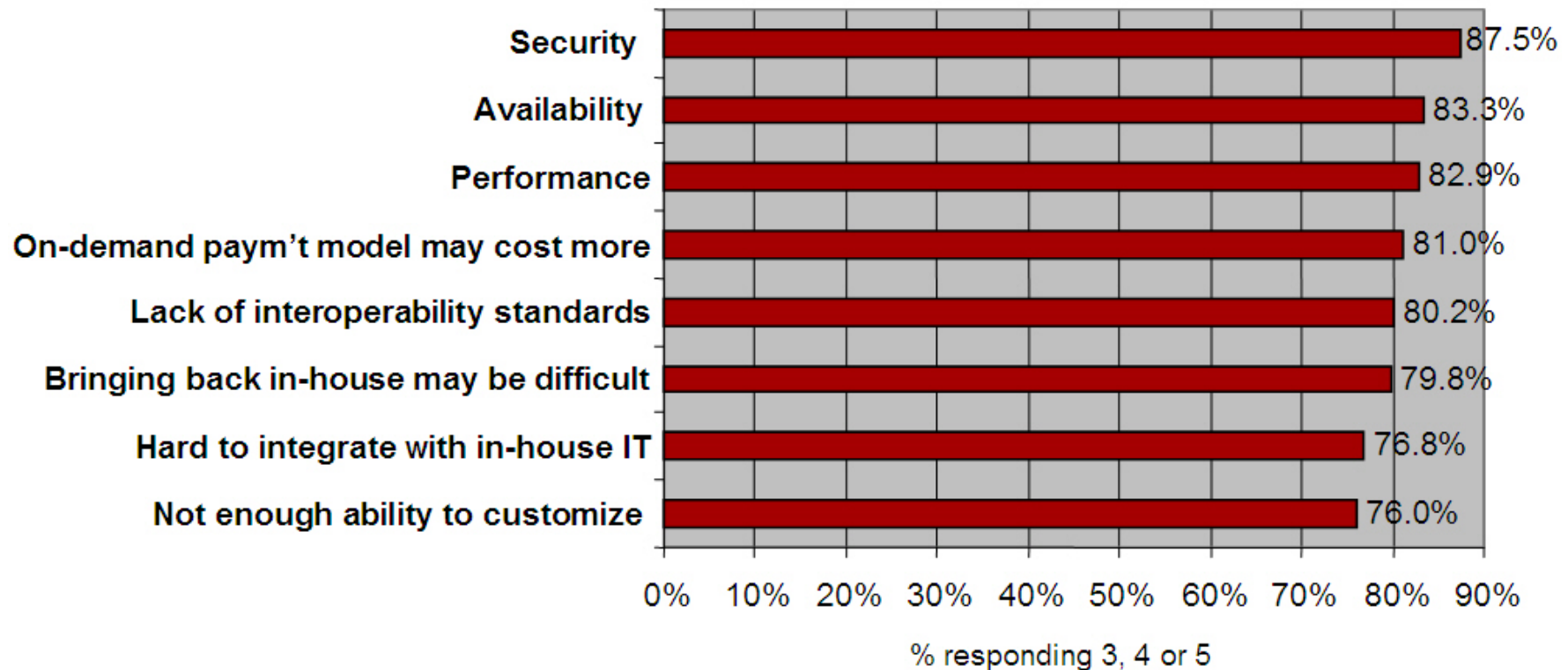
\* Assumed to incorporate subordinate layers.

# NIST Visual Model of Cloud Computing Definition



## Q: Rate the **challenges/issues** of the 'cloud'/on-demand model

(Scale: 1 = Not at all concerned 5 = Very concerned)



Source: IDC Enterprise Panel, 3Q09, n = 263

# Governance and compliance

## FY10 MS Online Data Centers and Markets

- Data Center location will be based on ship-to address during the purchase process
- Data will reside in 2 Data Centers to provide redundancy

■ Current market  
■ Coming in April 2010

- We have four datacenters in the US, two in Europe and two in Asia. Even though you choose to store your data in Europe instead of Worldwide, your data will be stored at least three times. Two times on your main location and one time at a secondary data center'



### Dublin with backup in Amsterdam

- |                   |                 |
|-------------------|-----------------|
| 1. Austria        | 13. Israel      |
| 2. Belgium        | 14. Netherlands |
| 3. Czech Republic | 15. Norway      |
| 4. Denmark        | 16. Poland      |
| 5. Finland        | 17. Portugal    |
| 6. France         | 18. Romania     |
| 7. Germany        | 19. Spain       |
| 8. Greece         | 20. Sweden      |
| 9. Hungary        | 21. Switzerland |
| 10. Ireland       | 22. UK          |

### Singapore with backup in Hong Kong++

- |                                 |
|---------------------------------|
| 1. Australia                    |
| 2. Hong Kong                    |
| 3. India (sales in Nov '09)     |
| 4. Japan                        |
| 5. Malaysia                     |
| 6. New Zealand                  |
| 7. Singapore (sales in Nov '09) |
| 8. South Korea (sales July '10) |
| 9. Taiwan (sales July '10)      |

++ Hong Kong will go-live in Oct 2009. APAC data will be backed up in the US until then

# Statement MS Azure:



Microsoft

**COMPUTERWORLD**

Subscribe to a Newsletter

Topics ▾NewsIn DepthReviewsBlogs ▾OpinionShark Tank

Government/  
IndustriesFinancial ServicesGov't Legislation/RegulationHealth CareIT Industries

[Home](#) > [Government/Industries](#) > [Gov't Legislation/Regulation](#)  
**News**  

## EU upset by Microsoft warning on U.S. access to EU cloud

By Jennifer Baker  
July 5, 2011 12:28 PM ET

1 CommentLike31

IDG News Service - Members of the European Parliament have demanded to know what lawmakers intend to do about the conflict between the European Union's Data Protection Directive and the U.S. Patriot Act.

The issue has been raised following [Microsoft's](#) admission last week that it may have to hand over European customers' data on a new [cloud](#) service to U.S. authorities. The company may also be compelled by the Patriot Act to keep details of any such data transfer secret. This is directly contrary to the European directive, which states that organizations must inform users when they disclose personal information.

"Does the Commission consider that the U.S. Patriot Act thus effectively overrules the E.U. Directive on Data Protection? What will the Commission do to remedy this situation, and ensure that E.U. data protection rules can be effectively enforced and that third country legislation does not take precedence over E.U. legislation?" asked Sophia In't Veld, a member of the Parliament's civil liberties committee.



# Amazon Outage

<http://aws.amazon.com/message/65648/>



AWS

Product

Sign in to the AWS Management Console

Quora

A continually improving collection of questions and answers created, edited, and organized by everyone who uses it.

## Summary of the Amazon EC2 Outage in the East Region

We're currently having an unexpected outage, and are working to get the site back up as soon as possible. Thanks for your patience.

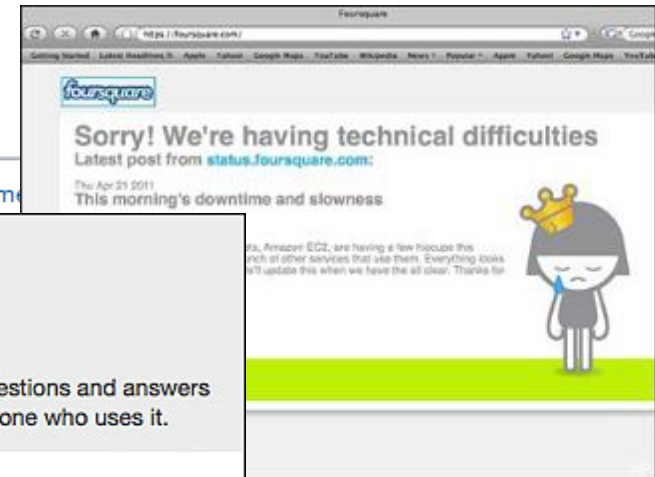
Amazon is currently experiencing a degradation. They are working on it. We are still waiting on them to get to our volumes. Sorry.

reddit is down.



involved a subset of the Amazon Elastic Block Store ("EBS") volumes in a single Availability Zone. Unable to service read and write operations. In this document, we will refer to these affected volumes to also get "stuck" when they attempted to read or write to the EBS cluster in that Availability Zone, we disabled all control APIs (e.g. CreateSnapshot) for EBS in the affected Availability Zone for much of the duration of the event. The degraded EBS cluster affected the EBS APIs and caused high error rates and latencies for EBS calls to those APIs across the entire EC2 East Region. As with any complicated operational issue, this one was caused by several root causes interacting with one another and therefore gives us many opportunities to protect the service against any similar event reoccurring.

ALEXANDRA  
INSTITUTET



# Account or Service Hijacking

- Zeus botnet running an unauthorized command and control center on Amazon's EC2 cloud computing

## Amazon Cloud has Dropped Malware Before

This past Wednesday, researchers discovered a [malicious website hosted on Amazon EC2](#) distributed via Amazon's cloud-computing service. Antivirus vendor Sophos

In the past three years, ScanSafe has recorded 80 unique malware incidents involving amazonaws, 45 of which were in 2009, 13 in 2008

Unlike real estate, when it comes to amazonaws should be treated as a source. On the plus side, when researchers find a stop to it. [As Amazon explains](#), Amazon EC2, make it easier for



## Zero Day

Ryan Naraine and Dancho Danchev

- Mobile
- RSS
- Email Alerts

33 Comments



Share



Print



Facebook



Twitter



Recommend

10 Votes

[Home](#) / [News & Blogs](#) / [Zero Day](#)

## Zeus crimeware using Amazon's EC2 as command and control server

By Dancho Danchev | December 9, 2009, 8:13am PST

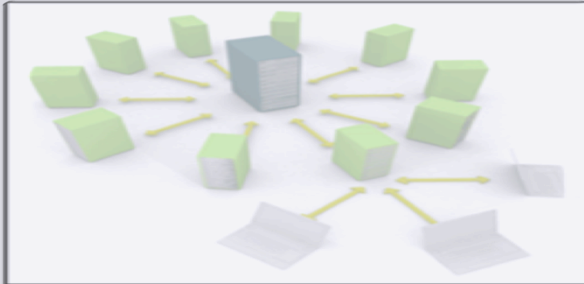
### Summary

A recently intercepted variant of the most popular piece of crime, the Zeus bot, is using Amazon's EC2 service as a command and control server.

Action	URL	Details
GET	http://ec2-170.compute-1.amazonaws.com/zeus/config.bin	svchost.exe
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe

**UPDATED:** ScanSafe posted an update stating that "In the past three years, ScanSafe has recorded 80 unique malware incidents involving amazonaws, 45 of which were in 2009, 13 in 2008, and 22 in 2007."

# Multi-Tenancy



## Multi-Tenancy

- one program, need to serve at the same time the number of consumer organizations (Tenants)



## Separation

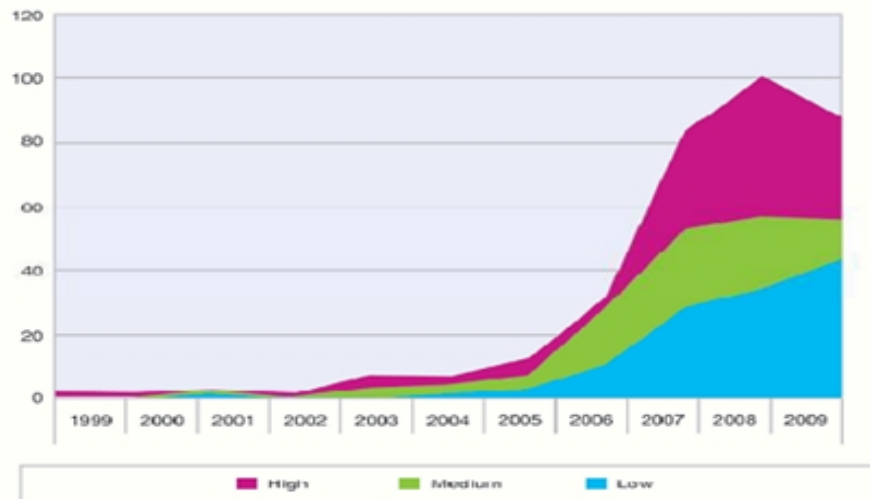
- Solution that supports Multi-Tenancy, capable of creating separation between the different Tenants

# Virtualization vulnerabilities by vendor

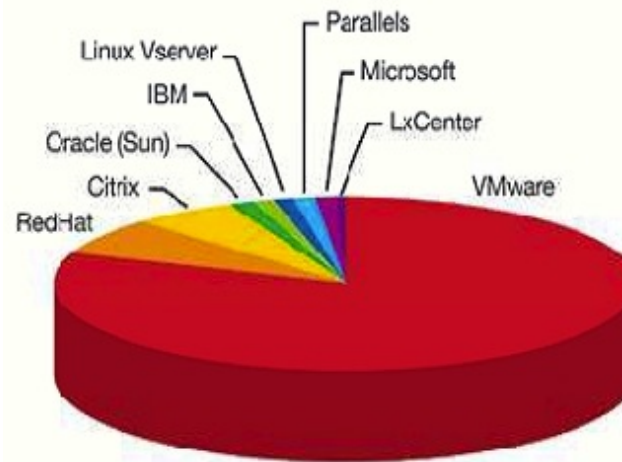
## Low percentages for Oracle, IBM, and Microsoft

- VMware: 80.9%
- Oracle: 1.8%
- RedHat: 6.9%
- IBM: 1.1%
- Citrix: 5.8%
- Microsoft: 0.9%

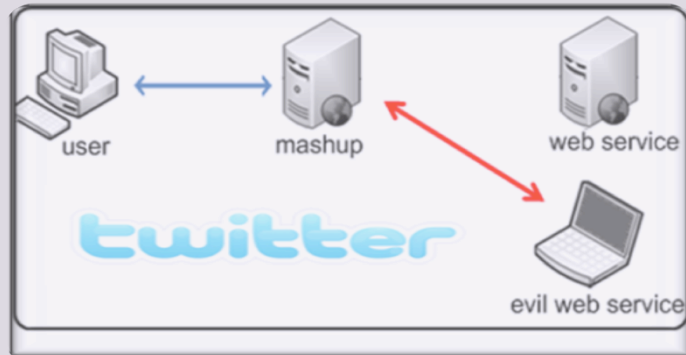
Virtualization Vulnerability Severity by Year Reported  
1999-2009



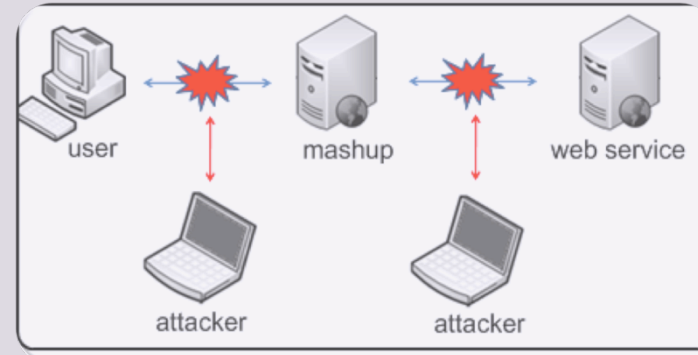
Virtualization Vulnerabilities by Vendor  
1999-2009



# Insecure Interfaces and APIs



*Web service  
redirection  
attack*



*Web service  
man-in-middle  
message  
alteration  
attack*



Here's both the old and the new language:

Old TOS:

Compliance with Laws and Law Enforcement. Dropbox cooperates with government and law enforcement officials and private parties to enforce and comply with the law. We will disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process (including but not limited to subpoenas), to protect the property and rights of Dropbox or a third party, to protect the safety of the public or any person, or to prevent or stop any activity we may consider to be, or to pose a risk of being, illegal, unethical, inappropriate or legally actionable.

New TOS:

Compliance with Laws and Law Enforcement Requests; Protection of Dropbox's Rights. We may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation, or legal request; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or its users; or (d) enforce our Terms of Service. If we provide your Dropbox files to a law enforcement agency, we will remove Dropbox's encryption from the files prior to providing them. However, Dropbox will not remove encryption from files that were encrypted prior to storing them on Dropbox.

More later

## 2.) Laws and U.S. law

The new TOS clarifies our commitment to user privacy. That said, there have been a lot of questions raised about government data requests.

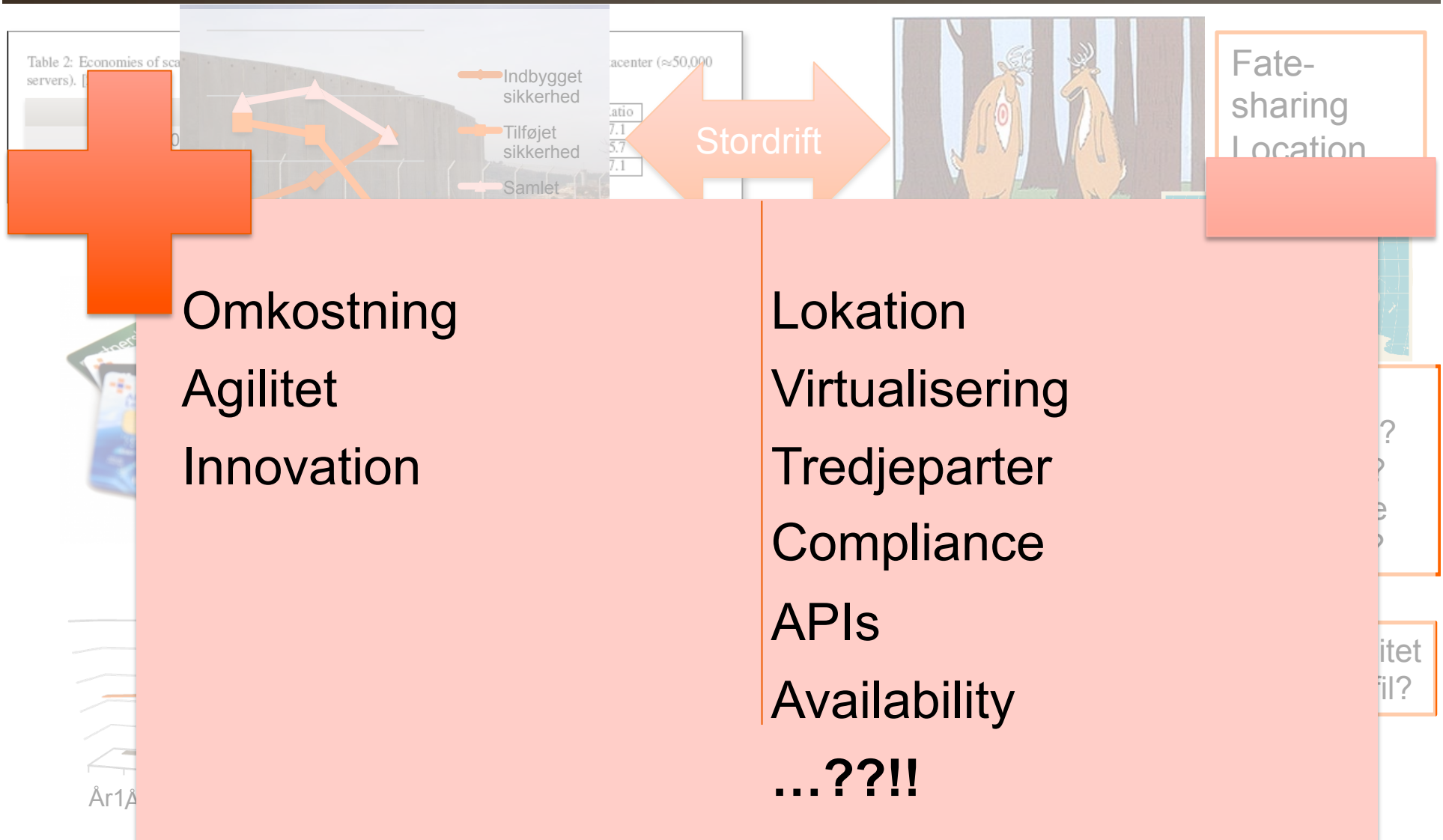
Just so you know, we don't get very many of those requests — about one a month over the past year for our more than 25 million users. That's fewer than one in a million accounts.

That said, like all U.S. companies, we must follow U.S. law. That means that the government sometimes requests us (as it does similar companies like Apple, Google, Skype, and Twitter) to turn over user information in response to requests for which the law requires that we comply.

When we get a government request, we don't just hand over your information or files. Our legal team vets all of these requests before we take any action. The small number of requests we have received have all been targeted to specific individuals under criminal investigation. If we were to receive a government request that was too broad or didn't comply with the law, we would stand up for our users and fight for their privacy rights.

**3.) We protect the privacy of users and will provide notice of government requests for data whenever possible**

# Business pros (and cons!)



# Cloud Security Alliance

The CSA  
organizes  
the use  
security  
Comput



## Welcome New Members

The CSA is a member-driven organization, chartered with promoting the use of best practices for providing security assurance within Cloud Computing. We would like to welcome our newest members:

- Credant
- BlueFire
- Alexandra Institute
- Lintasarta
- Sawis



[View all Members](#)

oting  
ding

cloud  
**CSA** security  
alliance<sup>SM</sup>

# Get certified!

## Certificate of Cloud Security Knowledge

The industry's first examination of cloud security knowledge.

### What the Industry Says

"The CSA Certificate of Cloud Security Knowledge (CCSK) will provide a consistent way of developing cloud security competency and... the confidence solutions."

~ Me

"The CSA, in... is challenging... thought-lea... safe and sec... CCSK, CSA is... and providing business executives a means to gauge the opinions and rhetoric associated with security in the cloud."

~ Jerry Archer, CSO, Sallie Mae

"The Certificate of Cloud Security Knowledge provides individuals with a solid foundation in cloud security issues and best practices. Organizations that leverage this

most out of... addition, the... tment efforts as... ence of an... ned the CCSK

assurance and  
Symantec Corp

an important step in improving security professionals' understanding of cloud security challenges and best practices and will lead to improved trust of and increased use of cloud services."

~ Matthew Gardiner, Director, CA Security Business

### CCSK Guidance V2.1

Cloud Architecture
Governance and Enterprise Risk
Legal and Electronic Discovery
Compliance and Audit
Information Lifecycle Management
Portability and Interoperability
Traditional Security, BCM, D/R
Data Center Operations
Incident Response
Application Security
Encryption and Key Management
Identity and Access Management
Virtualization

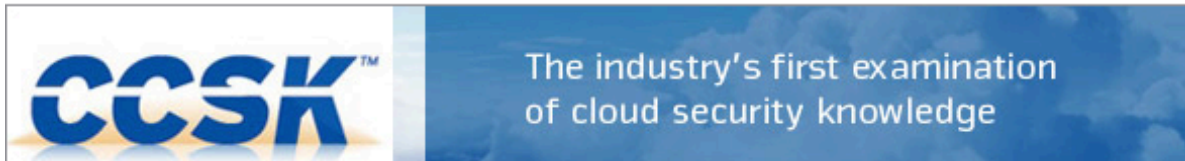



# Get certified!

## The Alexandra Institute offers a three-day course in Cloud Security

Get ready for CCSK certification.

Read here what [industry says](#).



Follow us on Facebook 

Stockholm 11.-13. october 2011  
Copenhagen 22.-24. november 2011

**Register**

**Call me**

### You will receive:

- Three-day training course by an [international expert](#)
- State-of-the-art knowledge about security and cloud computing
- Preparation for the CCSK exam
- Materials
- Test token providing access to examination at the Cloud Security Alliance (separate price \$ 300)
- Meals:
  - Lunch, coffee mornings and afternoons
  - Dinner at a restaurant on the second training day





Here's both the old and the new language:

Old TOS:

Compliance with Laws and Law Enforcement. Dropbox cooperates with government and law enforcement officials and private parties to enforce and comply with the law. We will disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process (including but not limited to subpoenas), to protect the property and rights of Dropbox or a third party, to protect the safety of the public or any person, or to prevent or stop any activity we may consider to be, or to pose a risk of being, illegal, unethical, inappropriate or legally actionable.

New TOS:

Compliance with Laws and Law Enforcement Requests; Protection of Dropbox's Rights. We may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that such disclosure is reasonably necessary to (a) comply with a law, regulation, or legal request; (b) protect the safety of any person from death or substantial physical injury; (c) prevent fraud or abuse of Dropbox or its users; or (d) enforce our Terms of Service. If we provide your Dropbox files to a law enforcement agency, we will remove Dropbox's encryption from the files prior to providing them to the agency. However, Dropbox will not remove encryption from files that were encrypted prior to storing them on Dropbox.

See Alon's technical paper

## 2. Compliance with Laws and U.S. law

The new TOS clarifies our commitment to user privacy. That said, there have been a lot of requests raised about government data requests.

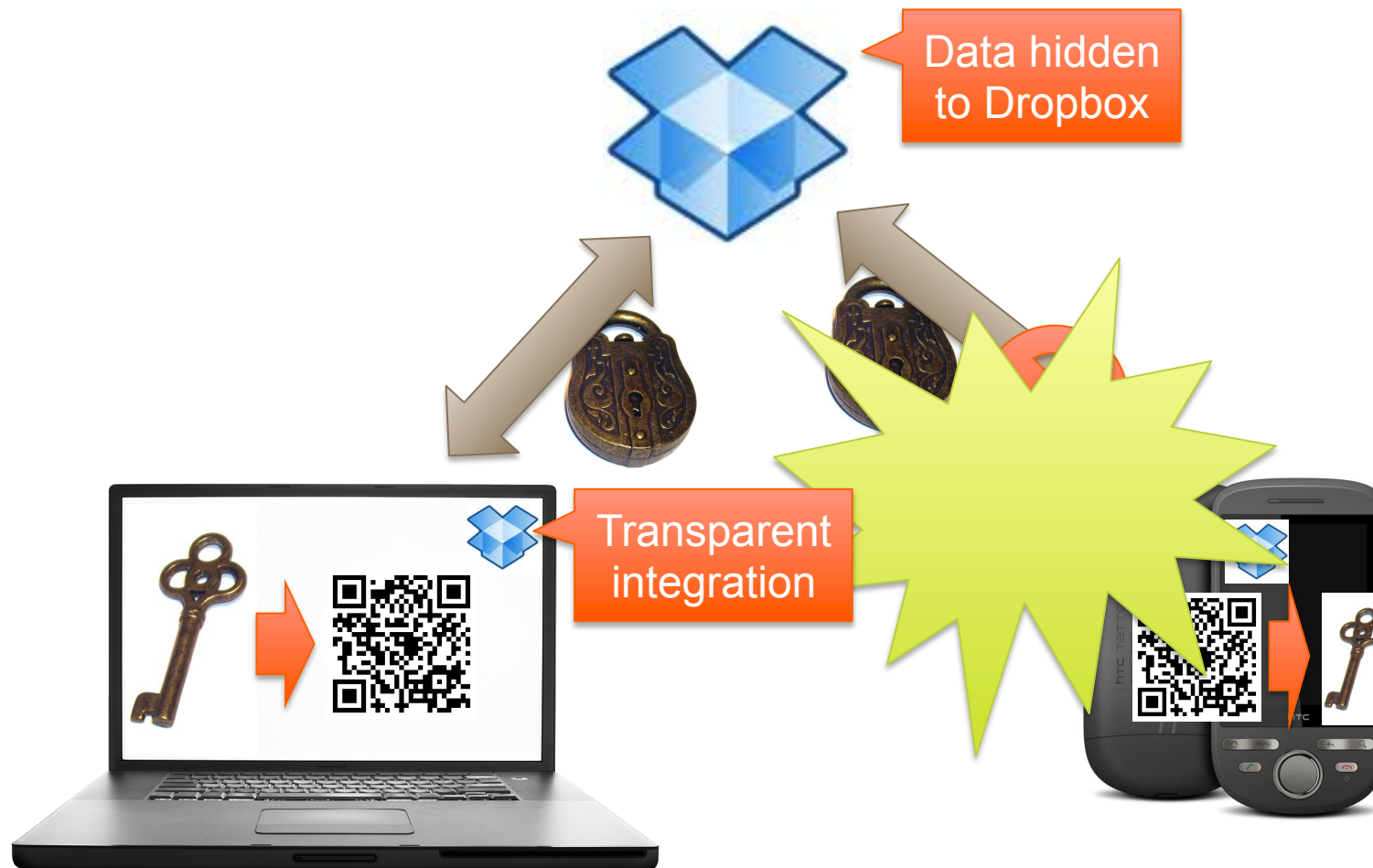
Just so you know, we don't get very many of those requests — about one a month over the past year for our more than 25 million users. That's fewer than one in a million accounts.

That said, like all U.S. companies, we must follow U.S. law. That means that the government sometimes requests us (as it does similar companies like Apple, Google, Skype, and Twitter) to turn over user information in response to requests for which the law requires that we comply.

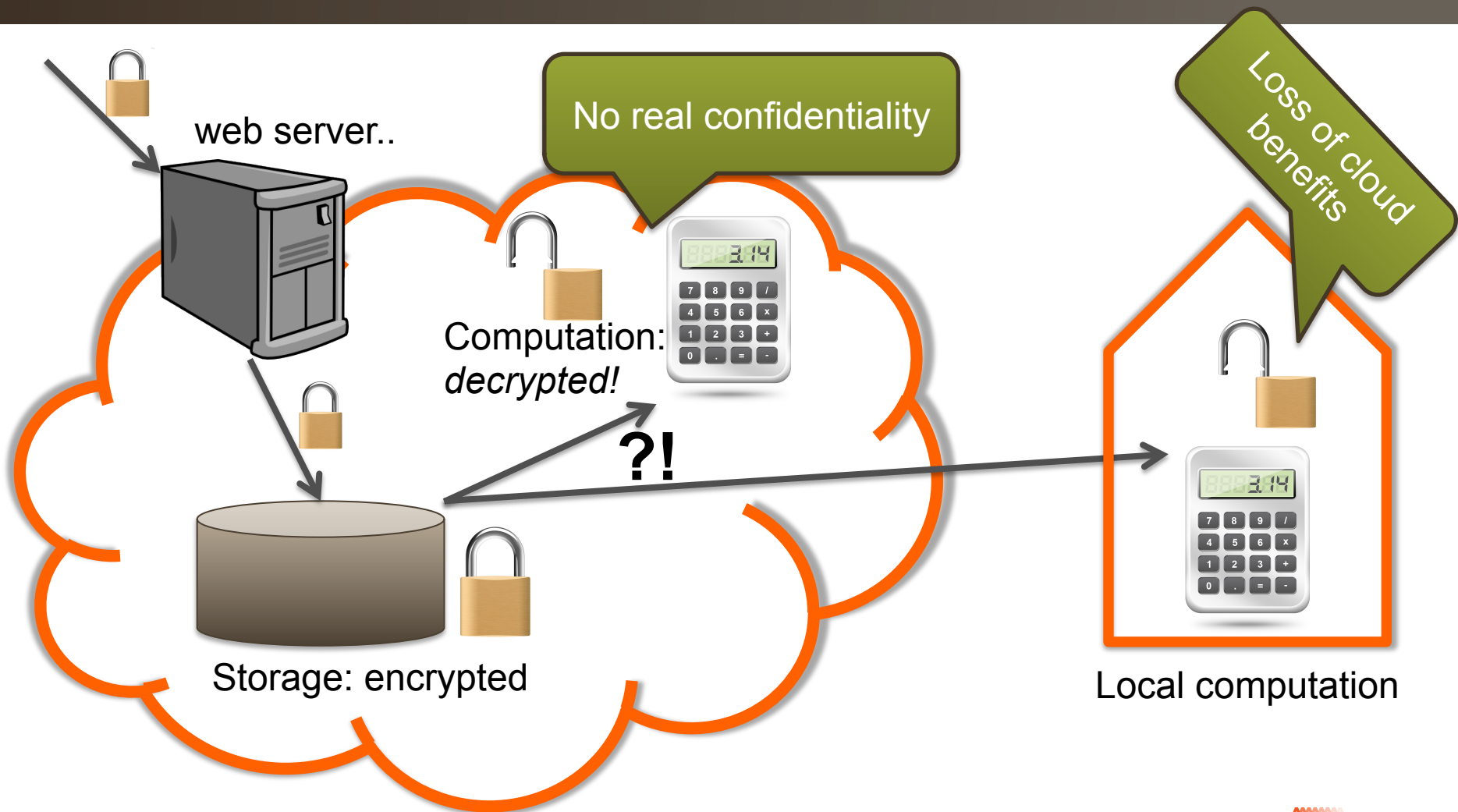
When we get a government request, we don't just hand over your information or files. Our legal team vets all of these requests before we take any action. The small number of requests we have received have all been targeted to specific individuals under criminal investigation. If we were to receive a government request that was too broad or didn't comply with the law, we would stand up for our users and fight for their privacy rights.

**3.) We protect the privacy of users and will provide notice of government requests for data whenever possible**

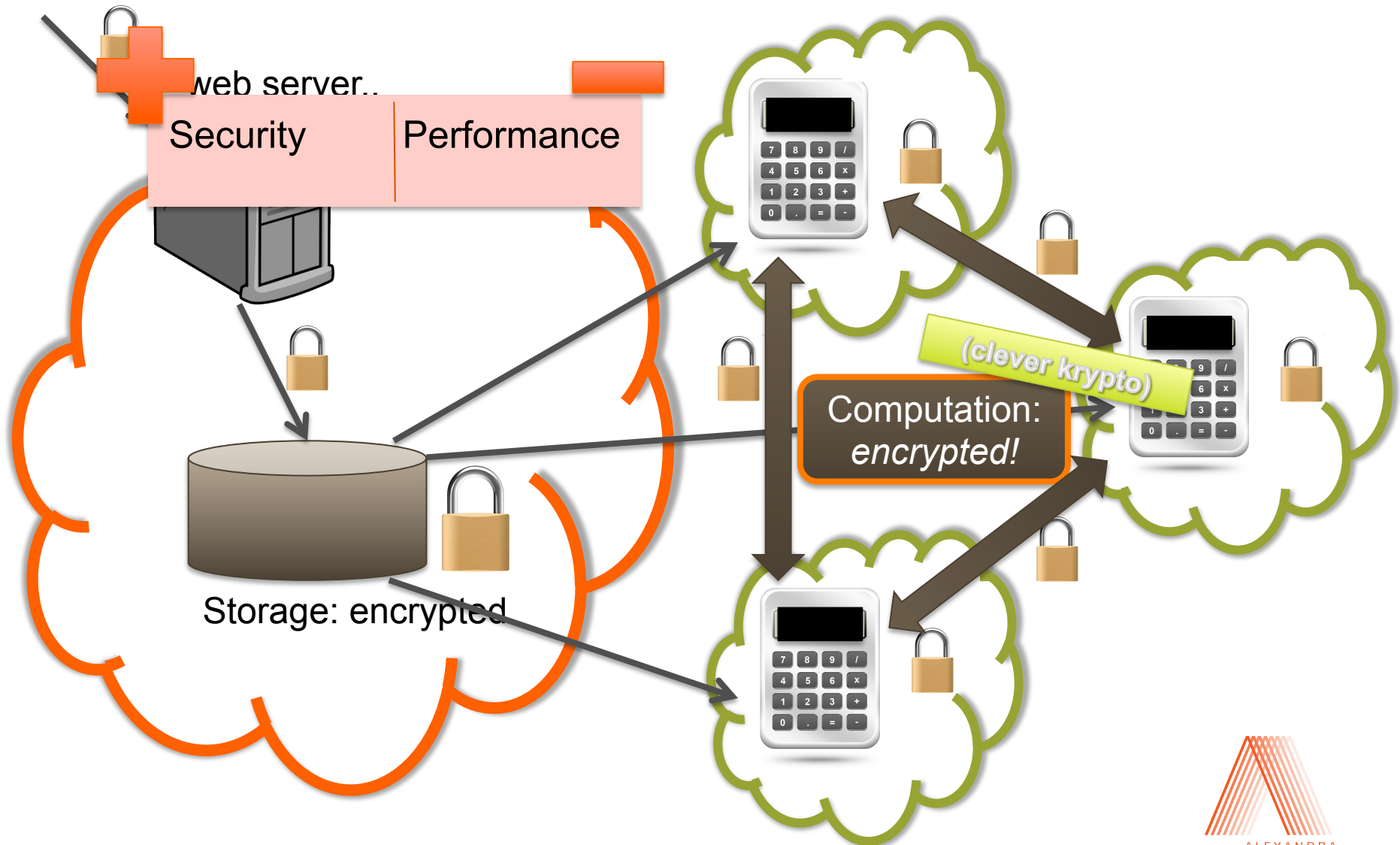
# A (proper) encrypted Dropbox



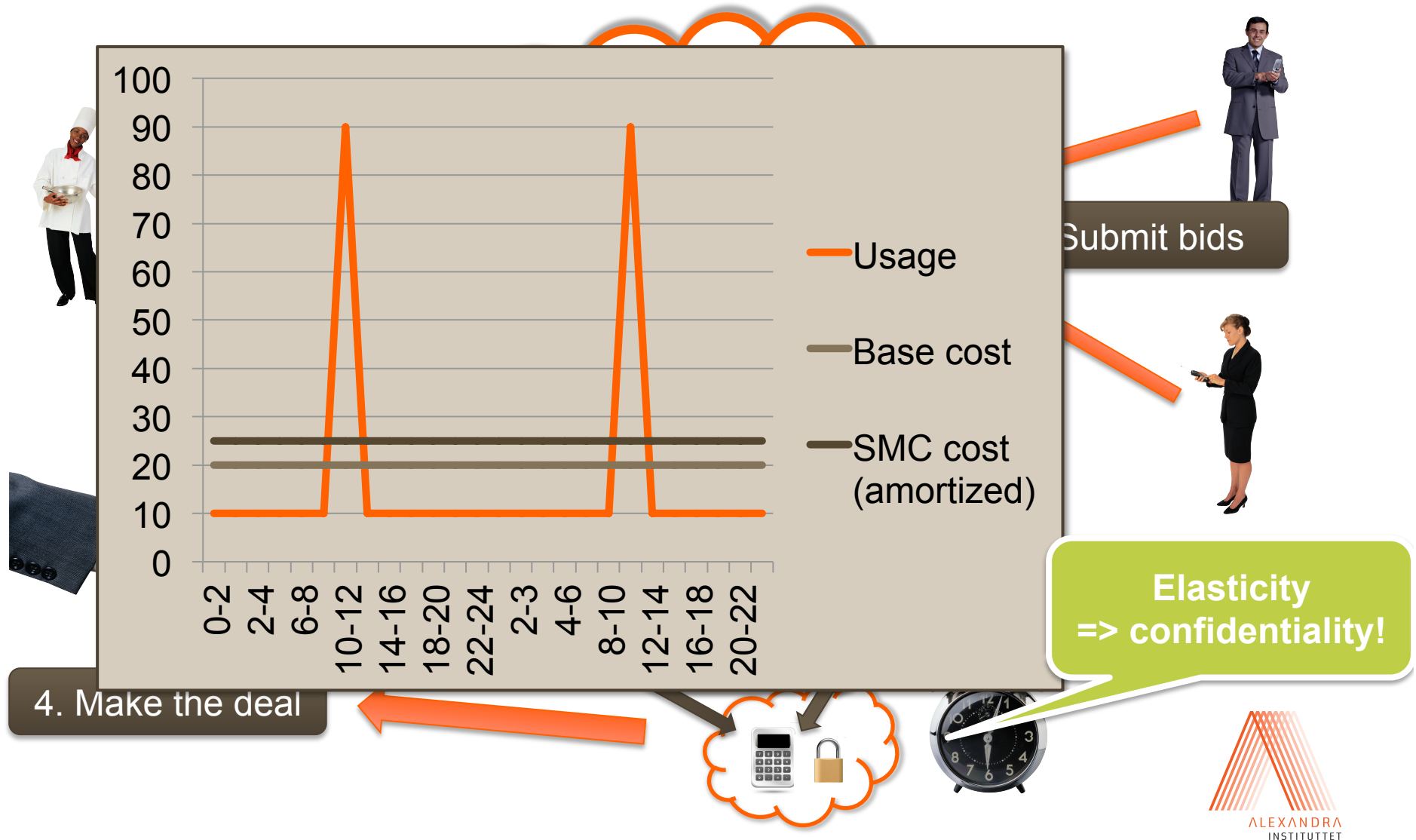
# Shallow confidentiality



# Deep confidentiality



# Case: energiauktion.dk (via partisia.com)



# Thx for you attention!



PS: Please remember to evaluate the presentations (incl. this one ;)