BITS Pilani presentation

BITS Pilani
Hyderabad Campus

D. Powar
Lecturer,
BITS-Pilani, Hyderabad Campus

innovate achieve lead

BITS Pilani
Hyderabad Campus

SSZG527

Cloud Computing

Agenda:

- Cloud security
  - Introduction to network security
  - Introduction to cloud security
  - Cloud security Issues
  - Threat Model
  - Top 5 cloud security threats
  - Who is responsible for managing security

Introduction

- Data on computers is an extremely important aspect of modern life. Therefore various areas in security began to gain prominence.

- Furthermore the internet took the world by storm and there were many examples of what could happen if there was insufficient security built in applications developed for the internet. Network security measures are needed to protect data during their transmission

SOURCE:NORTON REPORT 2013

WHO IS AFFECTED MOST BY CYBERCRIME?

CYBERCRIME VICTIMS MORE LIKELY TO BE:

MALE – 64% ♂

(COMPARED TO 58% OF FEMALES)

MILLENNIAL – 66%

(COMPARED TO 54% OF BABY BOOMERS)

AND:

- MOBILE DEVICE OWNERS – **63%**
- SOCIAL NETWORK USERS – **63%**
- PUBLIC / UNSECURED WI-FI USERS – **68%**
- EMERGING MARKET – **68%**
- PARENT OF CHILDREN 8-17 – **65%**

HIGHEST NUMBER OF CYBERCRIME VICTIMS FOUND IN:

RUSSIA

85%

CHINA

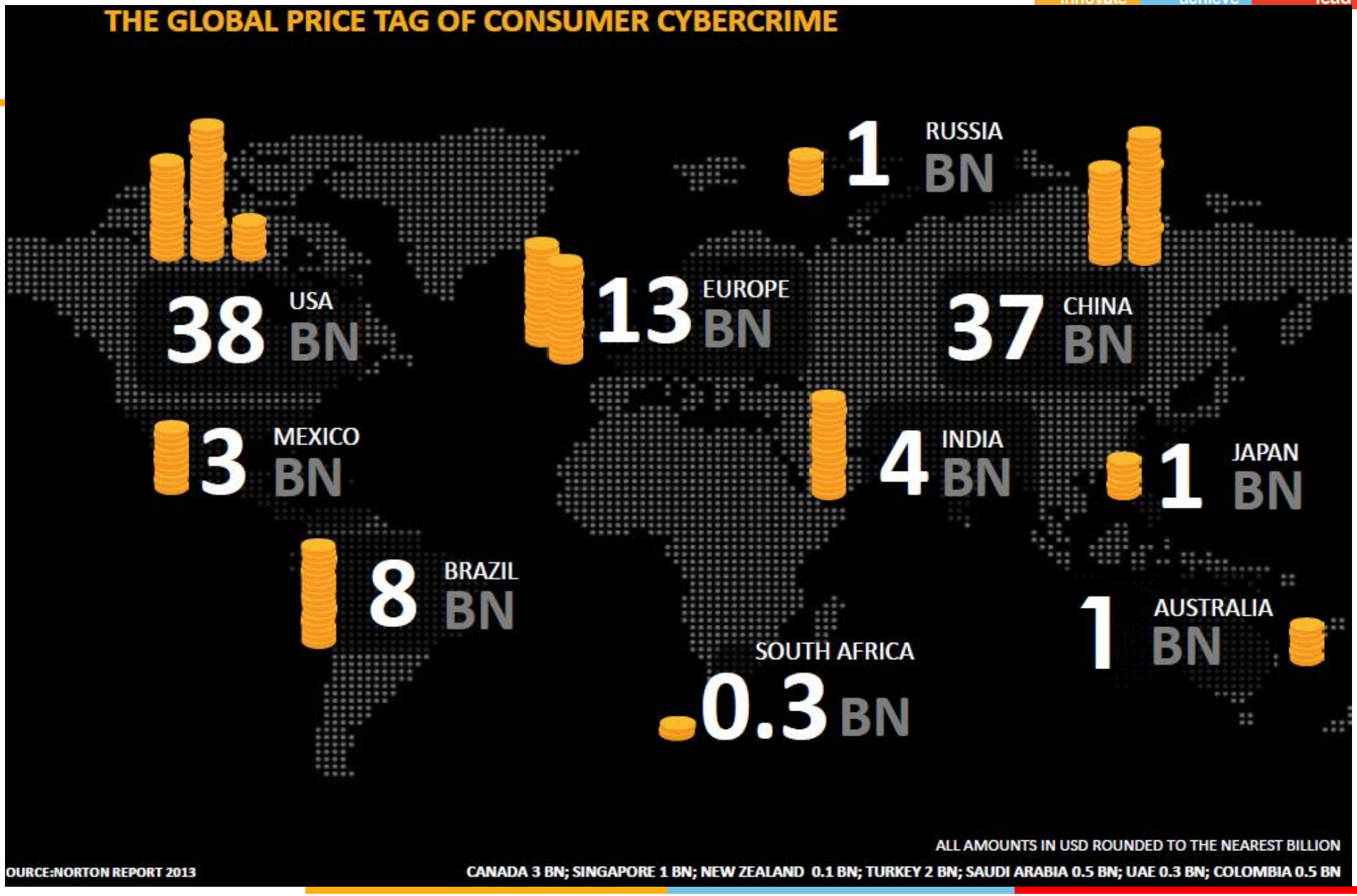
77%

SOUTH AFRICA

73%

USA 63%; CANADA 68%; UK 58%; FRANCE 45%; GERMANY 53%; ITALY 56%; SWEDEN 56%; POLAND 60%; NETHERLANDS 50%; AUSTRALIA 60%; INDIA 65%; JAPAN 19%; SINGAPORE 61%; NEW ZEALAND 69%; TURKEY 63%; DENMARK 50%; SAUDI ARABIA 62%; UAE 71%, COLOMBIA 64%

ALL STATS REFER TO LIFETIME VICTIMS


THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME
38 USA BN
1 RUSSIA BN
13 EUROPE BN
37 CHINA BN
3 MEXICO BN
4 INDIA BN
1 JAPAN BN
8 BRAZIL BN
1 AUSTRALIA BN
SOUTH AFRICA 0.3 BN
ALL AMOUNTS IN USD ROUNDED TO THE NEAREST BILLION
OURCE:NORTON REPORT 2013
CANADA 3 BN; SINGAPORE 1 BN; NEW ZEALAND 0.1 BN; TURKEY 2 BN; SAUDI ARABIA 0.5 BN; UAE 0.3 BN; COLOMBIA 0.5 BN

Different aspects of Information security

Security attacks:

- Any action that compromises the security of information owned by an organization.

Security mechanisms:

- A mechanism that is designed to detect, prevent or recover from a security attack.

Security services:

- A service that enhances the security of data processing system and the information transfers of an organization

Some general terms

- **Availability**: data/services can be accessed as desired
- **Integrity**: data has not been (maliciously) altered
- **Confidentiality**: no information has been inappropriately disclosed
- **Authentication**: user or data origin is properly identifiable
- **Accountability**: actions are traceable to those responsible

Security attacks

There are four categories of attacks

1. Interruption
2. Interception
3. Modification
4. Fabrication

A useful categorization of these attacks are in terms of passive attacks and active attacks

Security attacks

Interruption:

This is an attack on availability

Interception:

This is an attack on confidentiality

Modification:

This is an attack on integrity

Fabrication:

This is an attack on authenticity

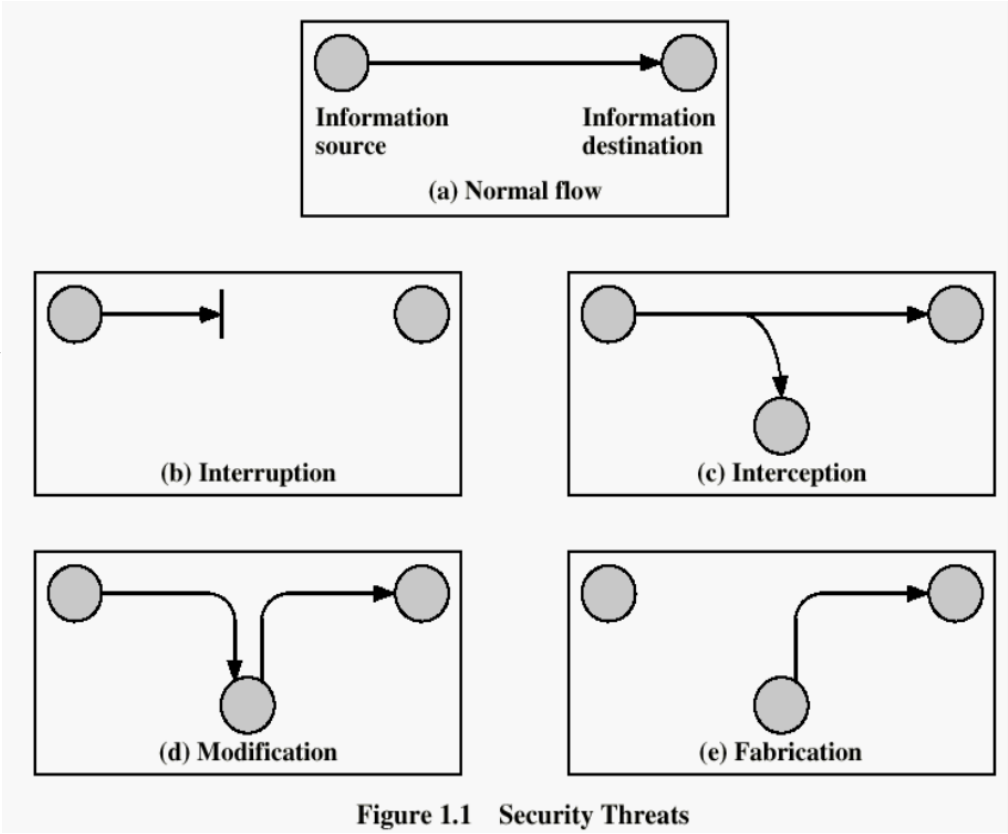


Figure 1.1 Security Threats

Goals of Security

Confidentiality

- Secrecy, privacy

Integrity

Availability

- Denial of service

Other goals

- Authenticity, non-repudiation,accountability, etc.

Passive Vs Active attacks

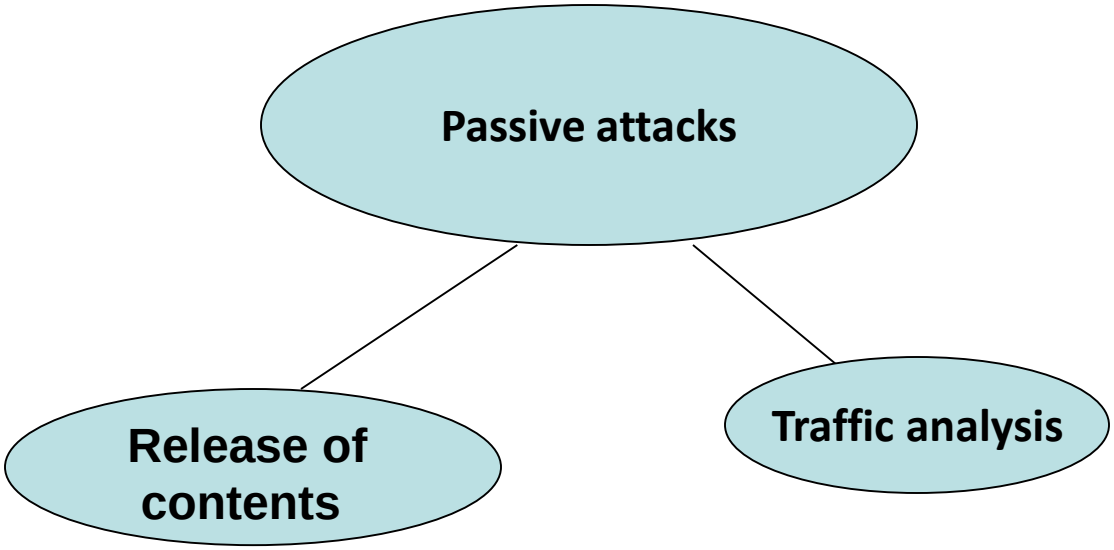
Passive:

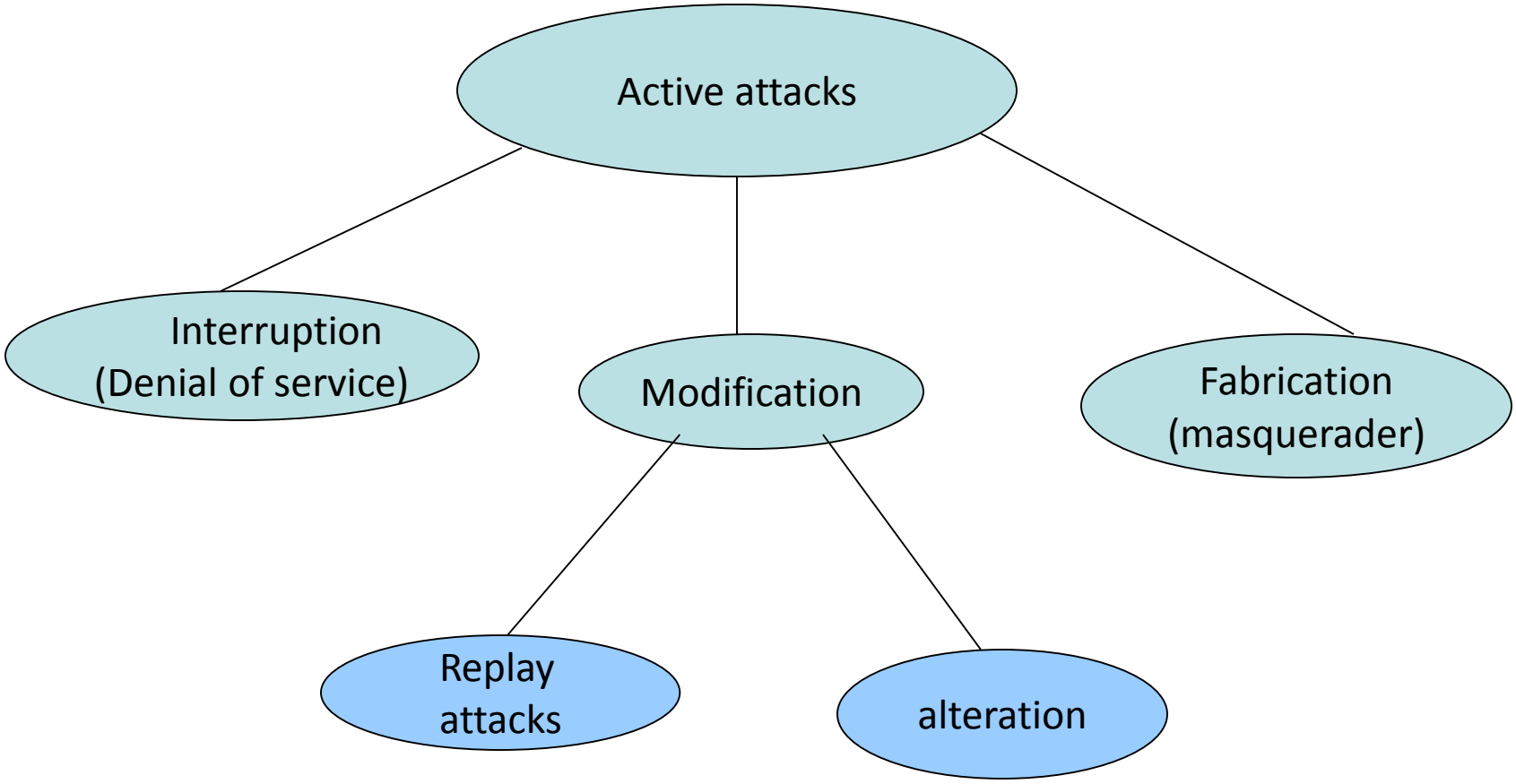
- Do not involve any modification to the contents of an original message.

Eg. An unauthorized party gain access to an asset(unauthorized copying of files or programs)

Active:

Contents of the original messages are modified in some way or a false message is created.


Passive attacks
Release of contents
Traffic analysis


Active attacks
Interruption
(Denial of service)
Modification
Fabrication
(masquerader)
Replay
attacks
alteration

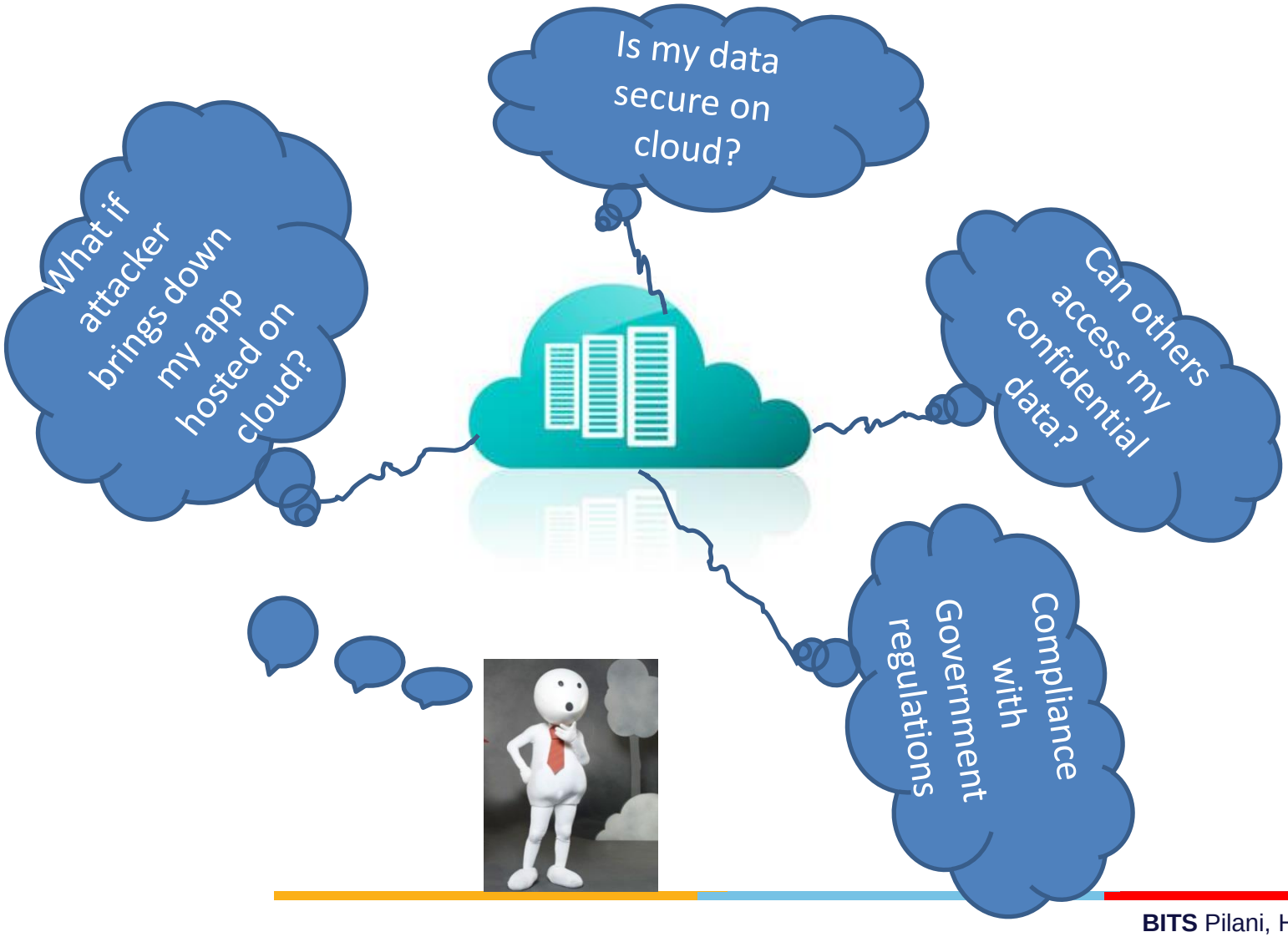
Security attacks in practice

Application level attack: The attacker attempts to access to information of a particular application or the application itself.

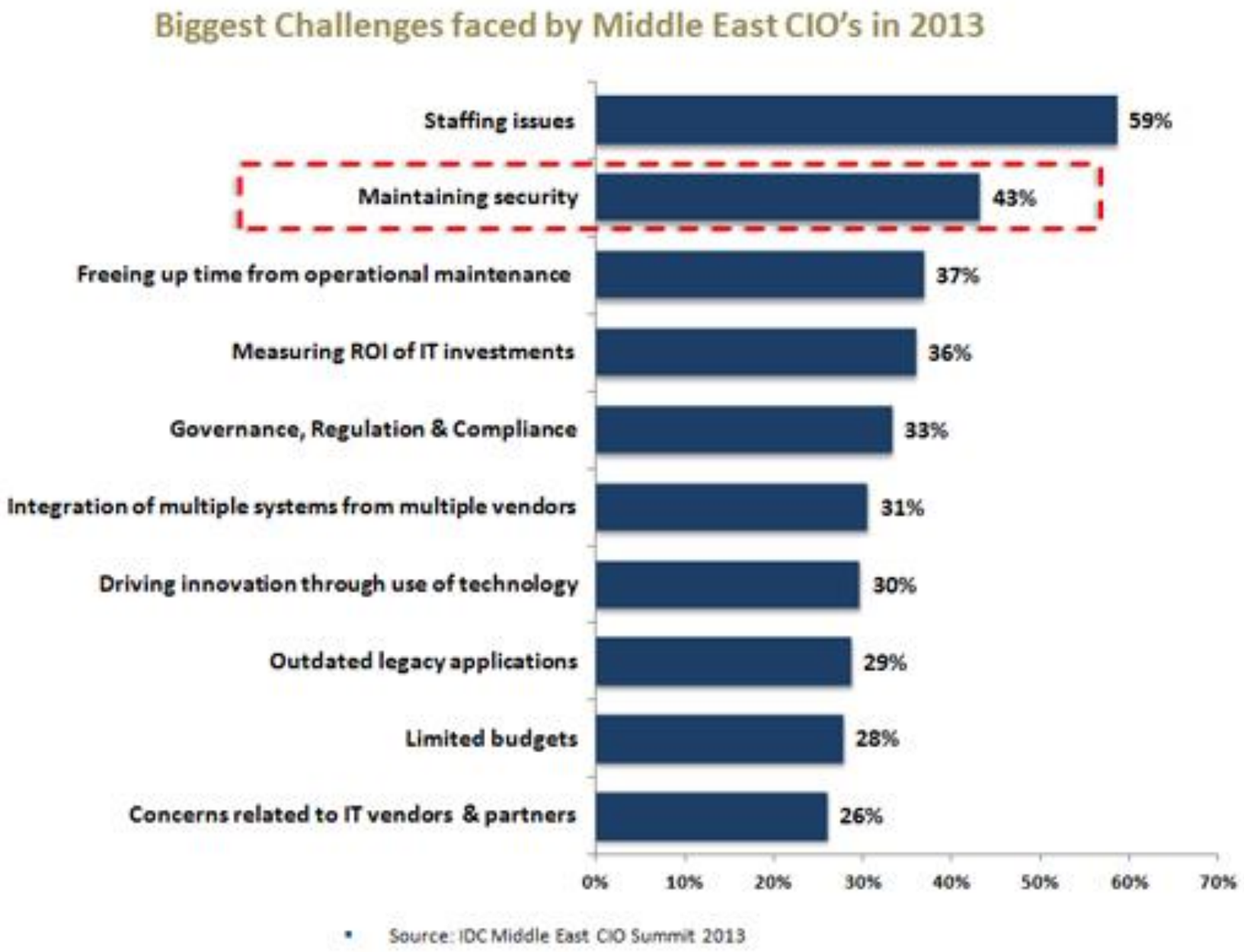
Network level attack: Aim at reducing the capabilities of a network by a number of possible means.

Introduction to cloud security

Security is the key inhibitor to cloud adaptation

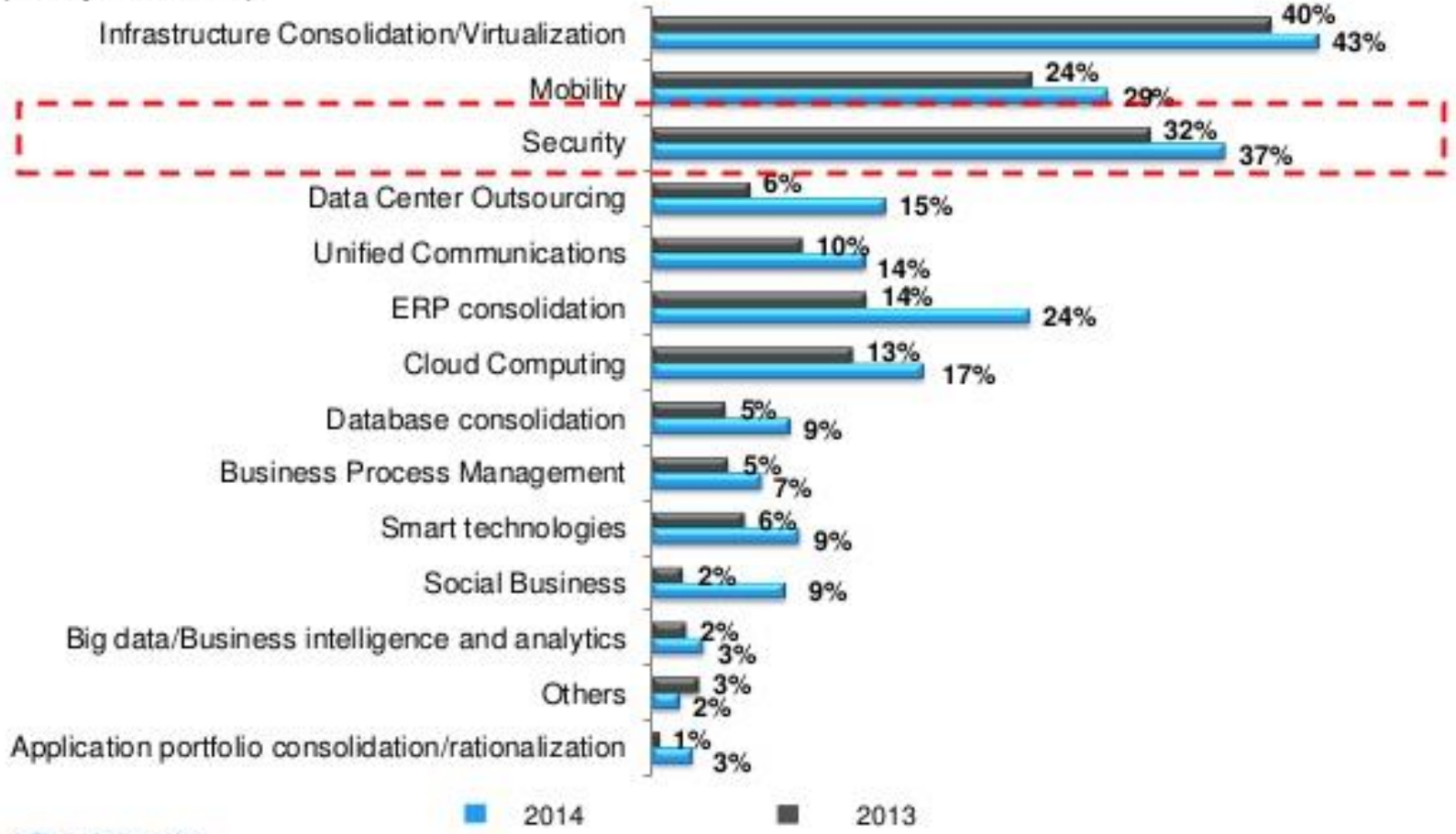


Companies are still afraid to use clouds

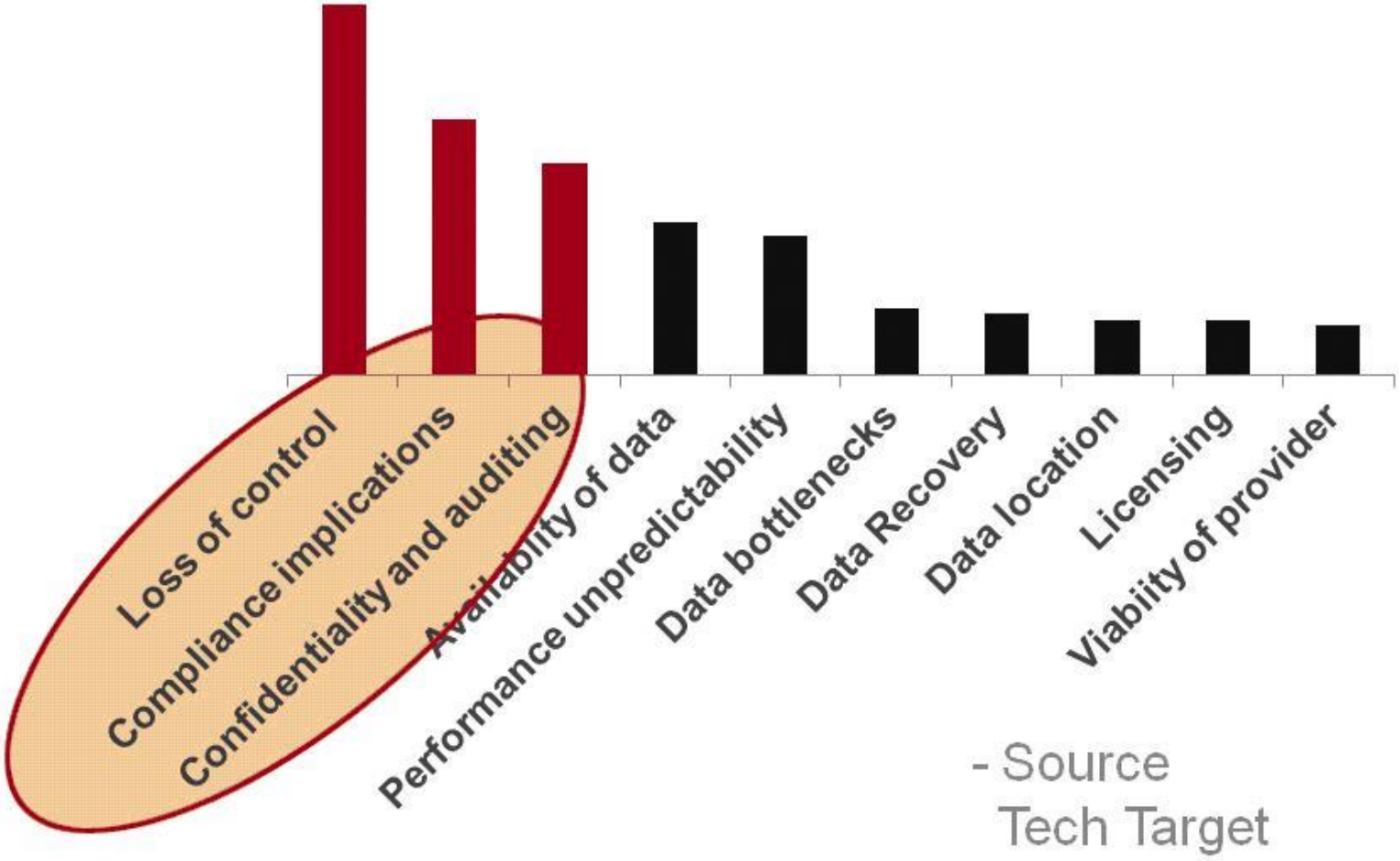


So far, investment in Security is becoming more proactive…

Q: *In the **next twelve months**, which of the following will be the **top IT initiatives** at your organization?* ***(Multiple Answer)***



Source: IDC Latin America IT Investment Trends January 2014 Latin America n=457 and IDC Latin America IT Investment Trends January 2013 Latin America n=592


Loss of control
Compliance implications
Confidentiality and auditing
Availability of data
Performance unpredictability
Data bottlenecks
Data Recovery
Data location
Licensing
Viabiity of provider
- Source
Tech Target

Recent Cloud attacks

innovate achieve lead

- Running of “Zeus botnet controller” on an EC2 instance on Amazon’s cloud infrastructure was reported in 2009
- iCloud hack
- Sony Pictures
- Home Depot
- Anthem

Problems Associated with Cloud Computing

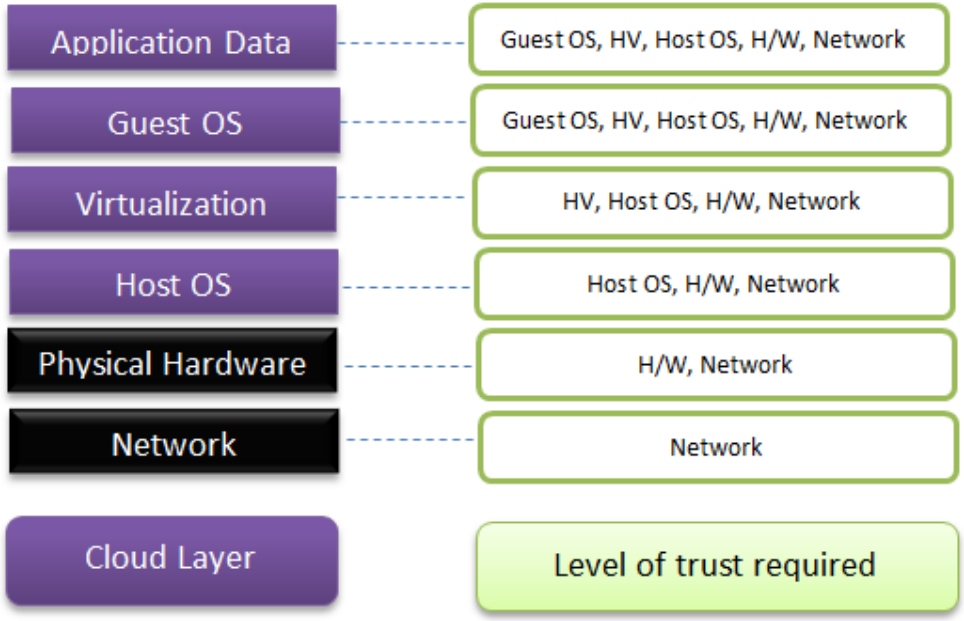
- Most security problems:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy
- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

Loss of Control in the Cloud

- Consumer's loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

Lack of Trust in the Cloud

- Trusting a third party requires taking risk
- Defining trust and risk
  - Opposite sides of the same coin (J. Camp)
  - People only trust when it pays (Economist's view)
  - Need for trust arises only in risky situations
- Trust here means mostly lack of accountability and verifiability



Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?
- Who are my neighbors? What is their objective?

Security Issues in the Cloud

In theory, minimizing any of the issues would help:

- Loss of Control
  - Take back control
    - Data and apps may still need to be on the cloud
    - But can they be managed in some way by the consumer?
- Lack of trust
  - Increase trust (mechanisms)
    - Technology
    - Policy, regulation
    - Contracts
- Multi-tenancy
  - Private cloud
    - Takes away the reasons to use a cloud in the first place
  - VPC: its still not a separate system
  - Strong separation

Minimize Loss of Control in the Cloud

- Monitoring
- Utilizing different clouds
- Access control management

Minimize Multi-tenancy in the Cloud

- Can't really force the provider to accept less tenants
  - Can try to increase isolation between tenants
    - Strong isolation techniques (VPC to some degree)
      - VM Side channel attacks (T. Ristenpart et al.)
    - QoS requirements need to be met
    - Policy specification
  - Can try to increase trust in the tenants
    - Who's the insider, where's the security boundary? Who can I trust?
    - Use SLAs to enforce trusted behavior

Threat Model

A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions

Steps:

- Identify attackers, assets, threats and other components
- Rank the threats
- Choose mitigation strategies
- Build solutions based on the strategies

Threat Model

Basic components

- Attacker modeling
  - Choose what attacker to consider
    - insider vs. outsider?
    - single vs. collaborator?
  - Attacker motivation and capabilities
- Attacker goals
- Vulnerabilities / threats

What is the issue?

- **The core issue here is the levels of trust**
  - Many cloud computing providers trust their customers
  - Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
  - The way that the cloud provider implements security is typically focused on the fact that those outside of their cloud are evil, and those inside are good.
- **But what if those inside are also evil?**

Security and Privacy Issues in Cloud Computing

Infrastructure Security

Data security and Storage security

Identity and Access Management (IAM)

Privacy

and more…

Infrastructure Security

Network Level

Host Level

Application Level

The Network Level

- Ensuring confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- Ensuring availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers

The Network Level - Mitigation

- Note that network-level risks exist regardless of what aspects of “cloud computing” services are being used
- The primary determination of risk level is therefore not which *aaS is being used
- But rather whether your organization intends to use or is using a public, private, or hybrid cloud.

The Host Level

SaaS/PaaS

- Both the PaaS and SaaS platforms abstract and hide the host OS from end users
- Host security responsibilities are transferred to the CSP (Cloud Service Provider)
  - *You do not have to worry about protecting hosts*
- However, as a customer, you still own the risk of managing information hosted in the cloud services.

Case study: Amazon's EC2 infrastructure

"Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds"

- Multiple VMs of different organizations with virtual boundaries separating each VM can run within one physical server
- "virtual machines" still have internet protocol(or IP), addresses, visible to anyone within the cloud.
- VMs located on the same physical server tend to have IP addresses that are close to each other and are assigned at the same time
- An attacker can set up lots of his own virtual machines, look at their IP addresses, and figure out which one shares the same physical resources as an intended target
- Once the malicious virtual machine is placed on the same server as its target, it is possible to carefully monitor how access to resources fluctuates and thereby potentially glean sensitive information about the victim

More on attacks…

- Can one determine where in the cloud infrastructure an instance is located?
- Can one easily determine if two instances are co-resident on the same physical machine?
- Can an adversary launch instances that will be co-resident with other user instances?
- Can an adversary exploit cross-VM information leakage once co-resident?
- Answer: Yes to all

Top 5 cloud security threats

1. Account hijacking
2. Insufficient Due Diligence
3. Data loss
4. Data breach
5. Insider threat

Account hijacking

- ✓ Multi-factor authentication
- ✓ Protect the global admin account

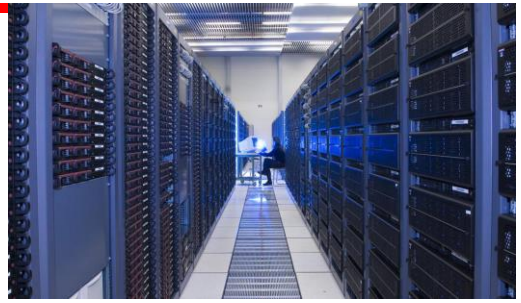
Insufficient Due Diligence

- Shadow IT (file sharing, social, collaboration, etc)
  - ✓ IT department need to be shepherds
  - ✓ Manageable services, access controls and encryption
  - ✓ User controls
  - ✓ Audit transparency

Data loss

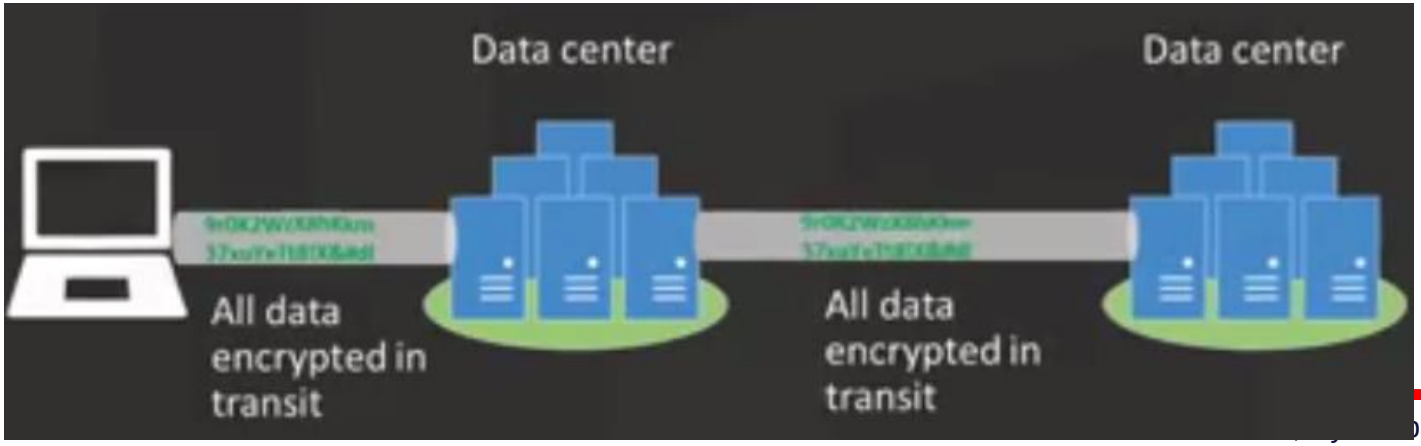
Accidental deletion

- Archiving service
- User / Admin level – recycle bin
- Can get data for a period of time (tombstoning)
- Redundancy for natural disasters (Geo-redundancy)



Data breach

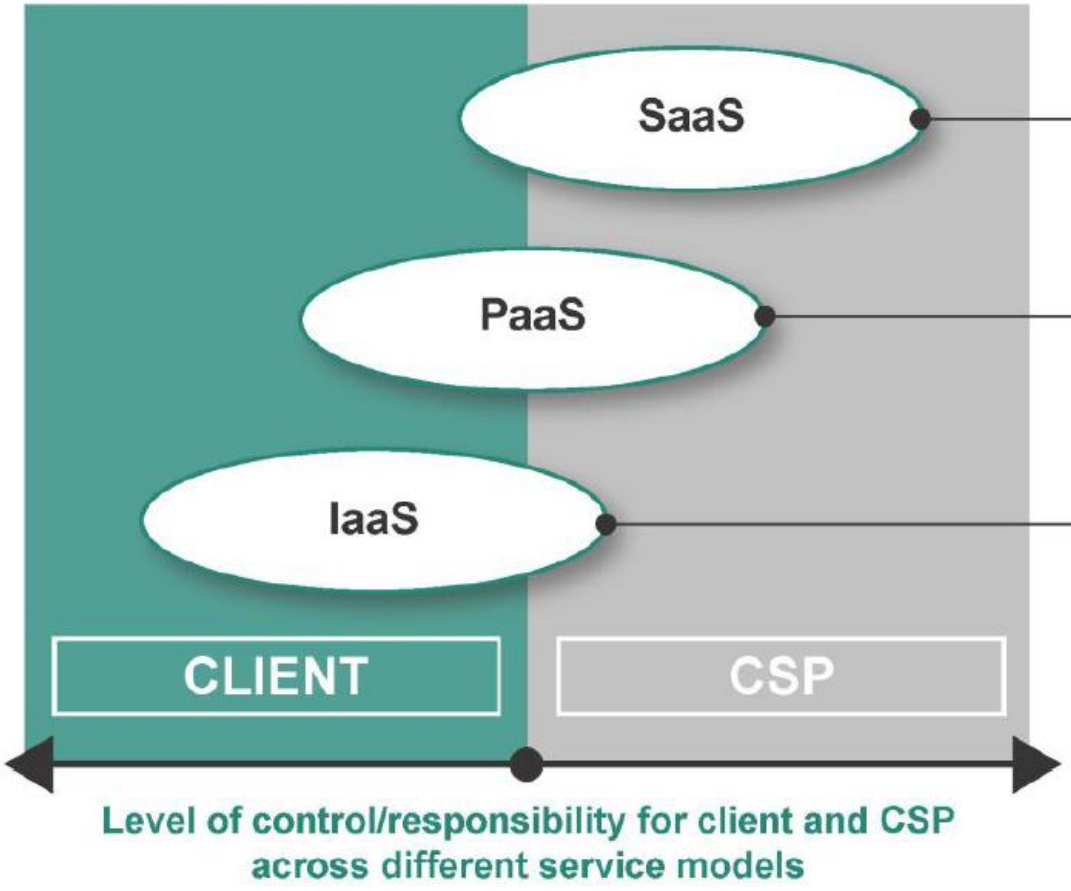
- **Media breach**
  - ✓ Physical security
  - ✓ Finding the data is like finding a needle in a haystack
  - ✓ Encryption at rest
- **Man in the middle**
  - ✓ Encryption in transit within and outside datacenters
  - ✓ End-to-end encryption
  - ✓ Message encryption



Malicious Insider (Insider threat)

- Least privilege access to operators
- Audit and monitor the admin accounts usage closely
- Elevations are granted with manual approval and for a limited period

Who is responsible for managing security



Level of control/responsibility for client and CSP across different service models

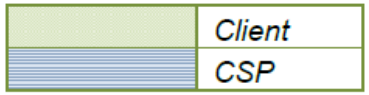
Saas
The client may have limited control of user-specific application configuration settings.

PaaS
The client has control over the deployed applications and possibly configuration settings for the application-hosting environment.

IaaS
The client has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Who is responsible for managing security (contd..)

Cloud Layer	Service Models		
	IaaS	PaaS	SaaS
Data	Client	Client	Client
Interfaces (APIs, GUIs)	Client	Client	CSP
Applications	Client	Client	CSP
Solution Stack (Programming languages)	Client	Client	CSP
Operating Systems (OS)	Client	CSP	CSP
Virtual Machines	Client	CSP	CSP
Virtual network infrastructure	Client	CSP	CSP
Hypervisors	CSP	CSP	CSP
Processing and Memory	CSP	CSP	CSP
Data Storage (hard drives, removable disks, backups, etc.)	CSP	CSP	CSP
Network (interfaces and devices, communications infrastructure)	CSP	CSP	CSP
Physical facilities / data centers	CSP	CSP	CSP



Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones
- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems

Summary

- Cloud security
  - Introduction to network security
  - Introduction to cloud security
  - Cloud security Issues
  - Threat Model
  - Top 5 cloud security threats
  - Who is responsible for managing security