ONLINECLOUDSEC.COM

# The Notorious 9

## Cloud computing Threats


**Moshe Ferber, CCSK**

Onlinecloudsec.com


ISACA Athens Annual Conference
Athens, Nov 2014

# About

- ✓ Information security professional for over 20 years
- ✓ Working on cloud strategy with the world largest software vendors
- ✓ Founded Cloud7, Managed Security Services provider (*currently 2bsecure cloud services)*
- ✓ Partner at Clarisite – ***Your customer's eye view***
- ✓ Partner at FortyCloud – ***Make your public cloud private***
- ✓ Member of the board at Macshava Tova – ***Narrowing societal gaps***
- ✓ Certified CCSK instructor for the Cloud Security Alliance.
- ✓ Co-Chairman of the Board, Cloud Security Alliance, Israeli Chapter

מחשבה טובה
Machshava Tova

cloud7
security simple.

CSAIL cloud security ISRAEL alliance℠

FORTYCLOUD
MAKE YOUR PUBLIC CLOUD PRIVATE

CLARISITE
YOUR CUSTOMER'S EYE VIEW

ONLINECLOUDSEC.COM

# What we are going to talk about?

**Cloud computing threats –**

what are they?

How do they reflect in the real world?

Which attacks vectors used?

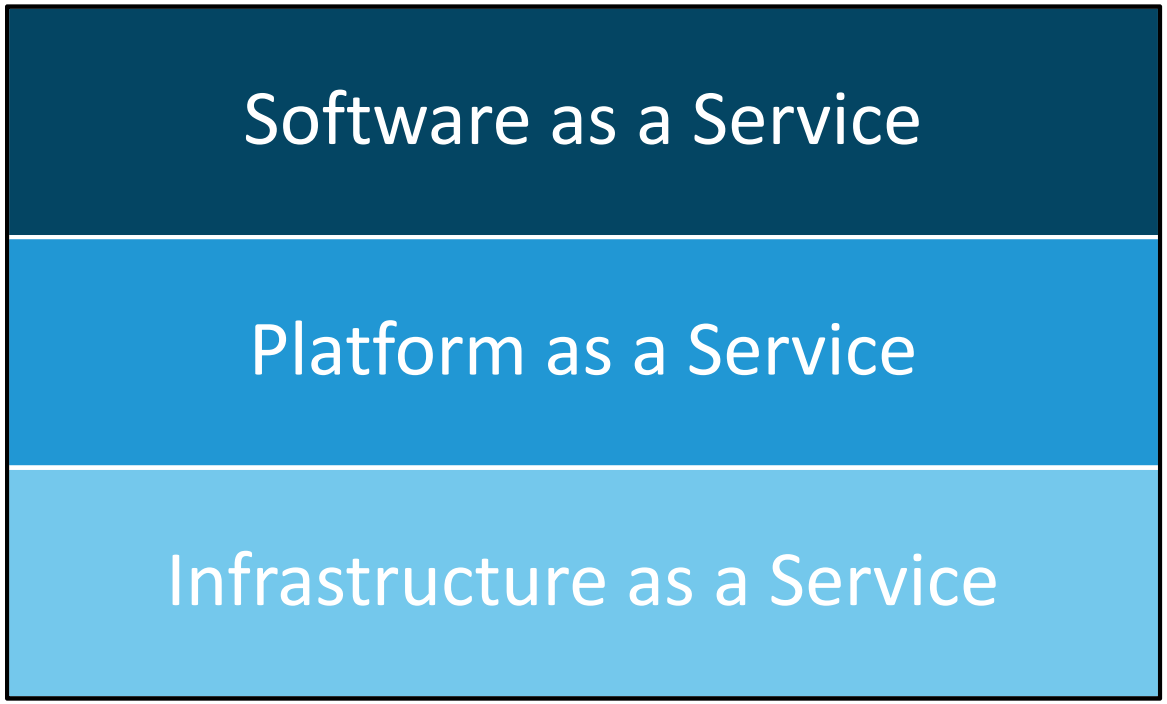
**Sources:**

- ✓ **Cloud Security Alliance** Notorious nine cloud computing threats.
- ✓ **Cloud Security Alliance** Cloud Computing Vulnerability Incidents: A Statistical Overview

ONLINECLOUDSEC.COM

# Cloud computing 2014 – what affects security?

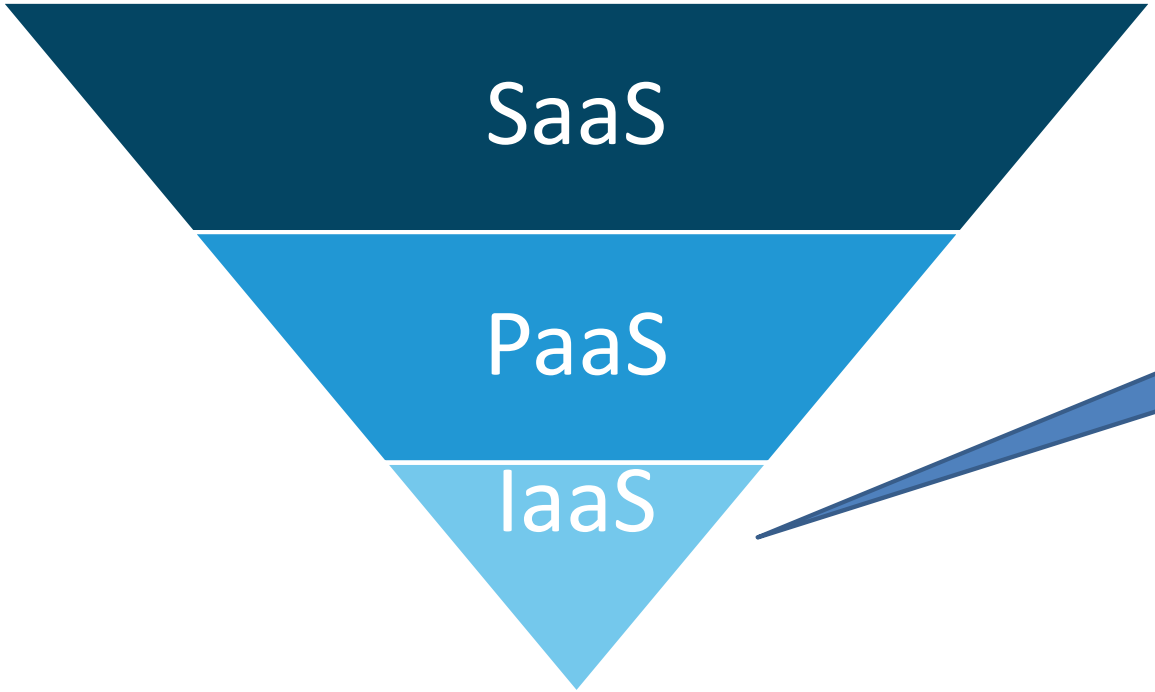
## We used to talk about cloud like this:




ONLINECLOUDSEC.COM

# Cloud computing 2014 – what affects security?

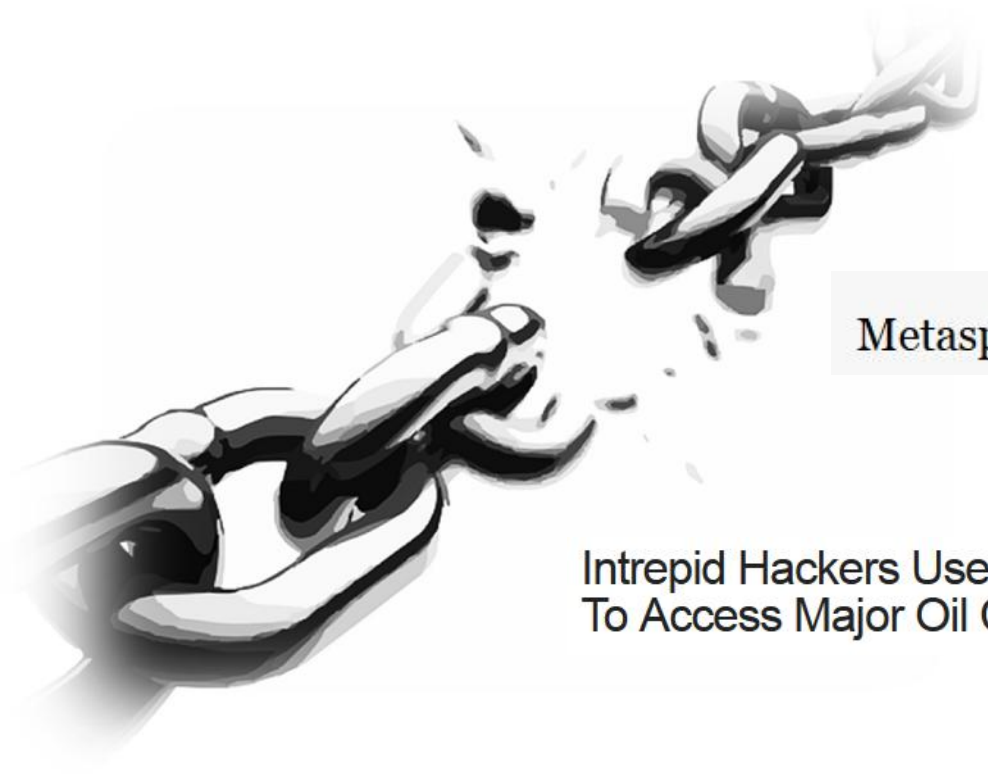
**But it is more like this:**




**Consolidation is growing at IaaS level**

ONLINECLOUDSEC.COM

# More supply Chain Attacks



**Target Hackers Broke in Via HVAC Company**

Metasploit's DNS Registrar Hacked Via Fax

Intrepid Hackers Use Chinese Take-Away Menu
To Access Major Oil Company

# The Cloud & Cyber

## Cloud Services Ransom Malwares


## Stealing CPU time

Crimeware-as-a-Service

ONLINECLOUDSEC.COM

# Moving on:

## The Notorious 9 Cloud computing Threats

ONLINECLOUDSEC.COM

# #1 Data Breaches

- ✓ Cloud Provider are targets for data breaches, sometimes just for the accounts details and not even for the data.
- ✓ iCloud, Evernote, Adobe tells the story well.
- ✓ But not all data lost happens due to hacking, Unintended disclosure is also happening.
- ✓ Cloud Computing and Shadow IT contribute to this phenomena.

**Adobe Breach Impacted At Least 38 Million Users**

iCloud Data Breach: Hacking And Celebrity Photos

Shadow IT


ONLINECLOUDSEC.COM

# #2 Data Lost

- ✓ **Hacking or simple failures – it does not really matter.**
- ✓ **Multi Cloud backup or external backups are not a "nice to have".**

How Apple and Amazon Security Flaws Led to My Epic Hacking

Oops! Dropbox Bug in Selective Sync Inadvertently Deletes Files

Utility Computing provider Flexiscale's Cloud appears to have floated away.

**Microsoft 'sorry' as Hotmail bug hits 17,000**

**Gmail users howl in anguish at 'disappeared' accounts**


ONLINECLOUDSEC.COM

# #3 Account Hijacking

## New account Hijacking Motivation:

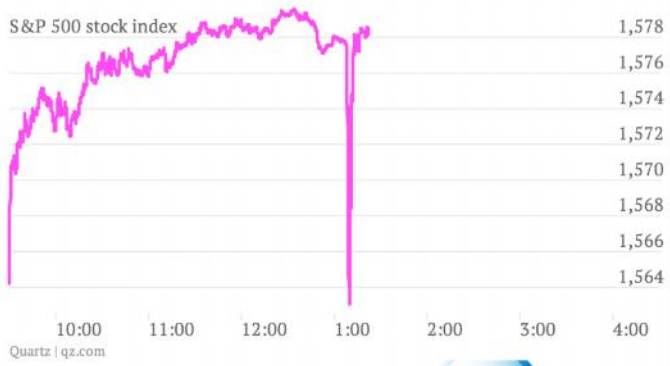

AP The Associated Press
@AP
Follow

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

483 RETWEETS 17 FAVORITES

10:07 AM - 23 Apr 13




NEWS

**Code Spaces forced to close its doors after security incident**

ONLINECLOUDSEC.COM

# #3 Account Hijacking

- ✓ **Most attacks used spear phishing.**
- ✓ **DNS ownership is also at attack vector**
- ✓ **Two factor & pro-active defenses for identifying account hijacking will continue.**
- ✓ **We will see more attacks on PaaS and on federation protocols.**

“ …the basic methods of gaining access to a victim’s environment are not. The most prolific is the old faithful: **spear phishing**. “

Verizon data breach report 2014

**Zeus bot found using Amazon's EC2 as C&C server**

ONLINECLOUDSEC.COM

# #4 Insecure Interfaces and API's

**The cloud providers management dashboard, especially in IaaS, is the most intimidating attack vector**

For the second time this year, someone has broken into Twitter's internal admin system and accessed accounts.

Why the Attack on Buffer Was a Serious Wake-Up Call for the Web

**OPENSSL HACKERS USED WEAK PASSWORD AT WEB HOST TO DEFACE SITE**


ONLINECLOUDSEC.COM

# #5 Denial of Service

- ✓ Network DDOS are becoming less common when talking about cloud providers.
- ✓ But application level attacks are increasing.

Wikileaks hit by second DDoS


DDoS attack against Bitbucket darkens Amazon cloud

**DNS Flood DDoS Attack**
*90 Million requests/sec (Above 110 Gbps)*

Cybercrooks use DDoS attacks to mask theft of banks' millions


ONLINECLOUDSEC.COM

# #6 Malicious Insider

**GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)**

**Fired techie created virtual chaos at pharma company**

Entire kids TV show deleted as former data hosting employee takes revenge

**Microsoft accuses former employee of cloud data theft**


ONLINECLOUDSEC.COM

# #7 Abuse of Cloud Services

## U.S. based Cloud Hosting providers contribute 44% of Malware distribution

**Twitter transformed into botnet command channel**

**PlayStation Network hack launched from Amazon EC2**

**Cloud economics strikes again**

Sudden FBI Raid claims Innocent Web Server – Is Your Website Next?

Attackers Using Dropbox and Wordpress to Target, Disguise and Distribute

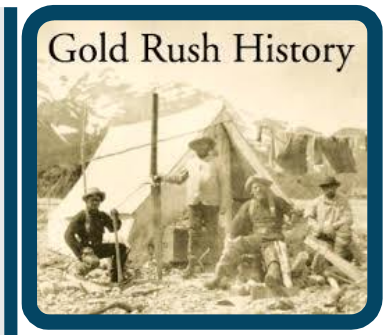
Megaupload user content safe for two more weeks

EFF joins battle to free user data from shuttered company's servers

ONLINECLOUDSEC.COM

# #8 Insufficient due Diligence

- ✓ Evaluating your provider is hard, very hard.
- ✓ Government legislation and industry efforts will lead to better understanding of Cloud Accountability.
- ✓ CSA will help in promoting transparency and provider evaluation methodology.





Eli Lilly dumps Amazon Web Services over legal struggle

Nirvanix cloud customers face worst nightmares

You have 2 weeks to pickup your cloud


ONLINECLOUDSEC.COM

# #8 Insufficient due Diligence

- ✓ Transparency is a key feature for trust.
- ✓ Government legislation and industry efforts will lead to better understanding of Cloud Accountability.
- ✓ CSA will help in promoting transparency and provider evaluation methodology.

ONLINECLOUDSEC.COM

# #9 Shared Technologies vulnerabilities

**Zoho users logging into other accounts by accident**

**Windows Live suffers user details identity crisis**

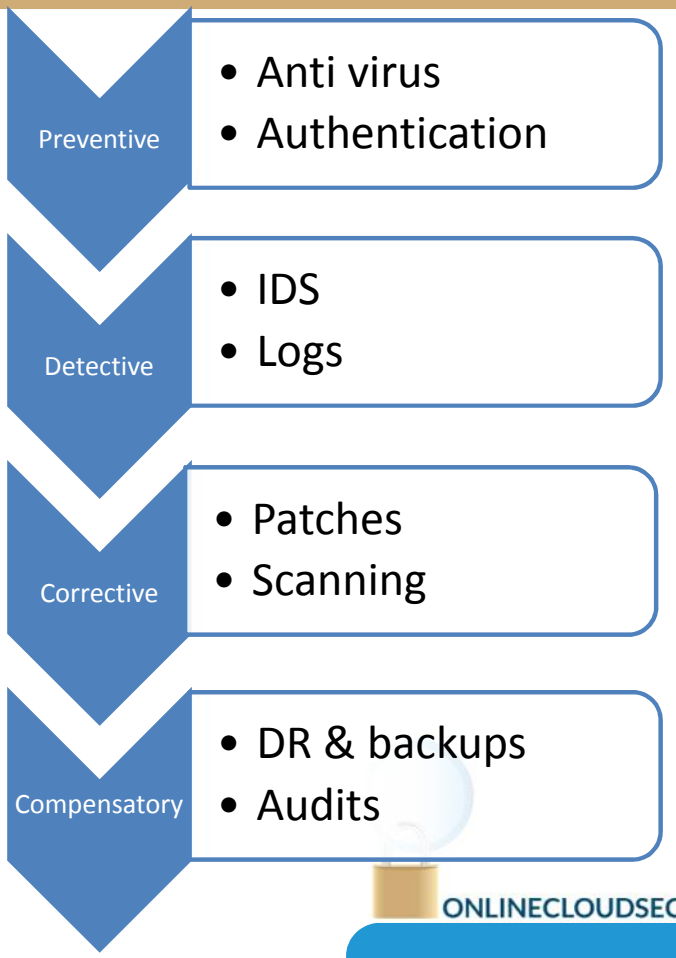
Cloud file-hosting service Dropbox leaves 25m users' accounts unlocked for four hours

**New Virtualization Vulnerability Allows Escape To Hypervisor Attacks**


ONLINECLOUDSEC.COM

# Recommendation for Cloud Consumers

- ✓ **Invest in education.**
- ✓ **Establish Cloud Strategy.**
- ✓ **Decide what is going to the cloud, and under which controls.**
- ✓ **Invest in technologies to help you maintain control of your data.**
- ✓ **Learn how to audit your provider, his services and the supply chain.**



# KEEP IN TOUCH

ONLINECLOUDSEC.COM


## Moshe Ferber

moshe@onlinecloudsec.com

www.onlinecloudsec.com

LinkedIn

http://il.linkedin.com/in/MosheFerber


**Cloud Security Course Schedule can be find at:**

**http://www.onlinecloudsec.com/course-schedule**