New Security Challenges Facing Cloud and Mobile Expansion

Aiuken Solutions

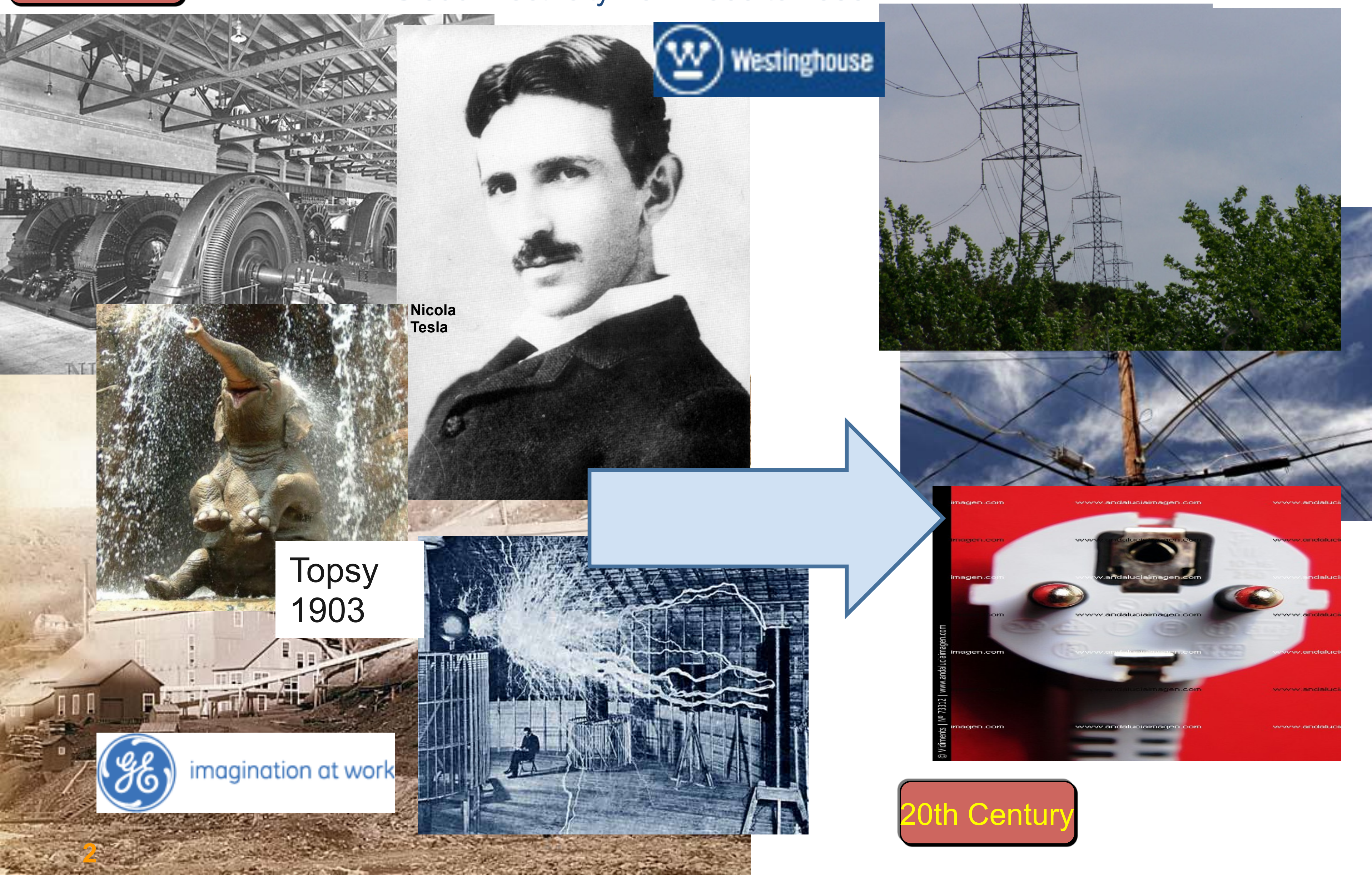
Juan M. Velasco,

CEO, Aiuken Solutions.Spain

19th Century

01 The War of Currents: AC / DC

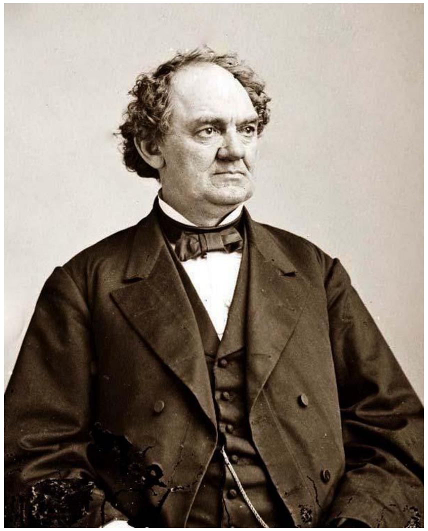
Cloud Electricity from 1900 to 1930



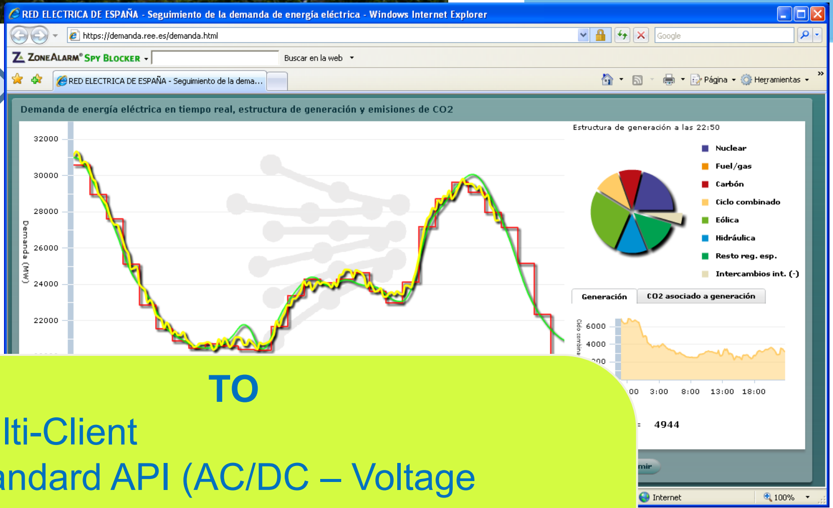
20th Century

01 Cloud Introduction– Electricity Cloud

Electricity revolution vs Cloud Revolution



1890 – Anonymous Enterprise:
“Our Business doesn’t need any external current at all, we are autonomous”



RED ELECTRICA DE ESPAÑA - Seguimiento de la demanda de energía eléctrica - Windows Internet Explorer
https://demanda.ree.es/demanda.html
Google
ZoneAlarm® Spy Blocker
Buscar en la web
RED ELECTRICA DE ESPAÑA - Seguimiento de la dema...
Página
Herramientas
Demanda de energía eléctrica en tiempo real, estructura de generación y emisiones de CO2
32000
30000
28000
26000
24000
22000
Demanda (MW)
Estructura de generación a las 22:50
Nuclear
Fuel/gas
Carbón
Ciclo combinado
Eólica
Hidráulica
Resto reg. esp.
Intercambios int. (-)
Generación
CO2 asociado a generación
6000
4000
3:00
8:00
13:00
18:00
4944
Internet
100%

FROM

- No multi-client
- Limited Generation
- No standardization
- High investment required
- Dedicated technical team required
- Local scope

TO

- Multi-Client
- Standard API (AC/DC – Voltage 110V-220V)
- Pay – per – Use
- 24x7 always on
- Remote management & support
- Unlimited service
- Worldwide service

http://www.ree.es/operacion/curvas_demanda.asp

How to find eficency with IT infrastructures?

IT evolution Cloud as IaaS / SaaS

IT Infrastructures

Aplications

SW Base & Middleware

IT Equipment

DataCenter Infrastructures

First Approach to Cloud

Manteinance consolidation
Operations consolidation

Support Considation
Standarazation
Software free

HW Consolidation
Virtualization

Cooling Consolidation
Free Cooling
Cold / Warm corridor

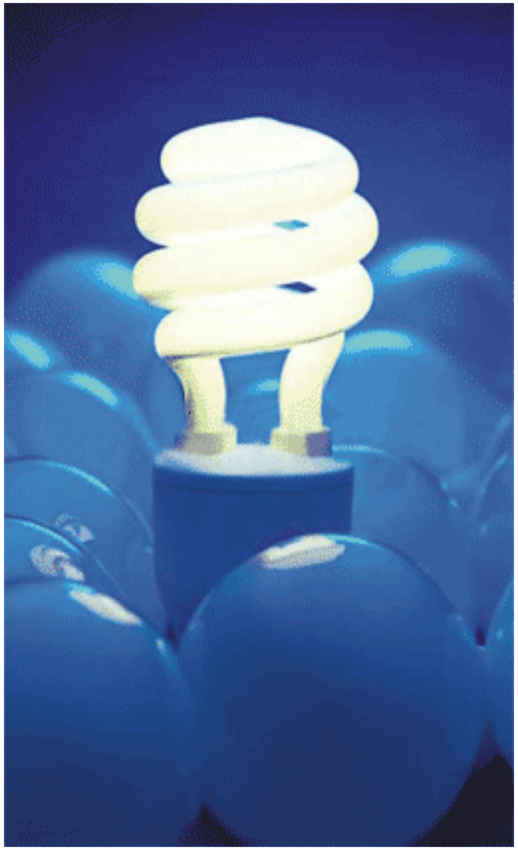
Transformation

SaaS
IaaS
Services Centers

Private Cloud
(Sharing for Gov only)

DataCenter Consolidation

Cloud answer for: Efficiency?



Standards?

Interoperativity?

roll back?

SLAs?

Pricing?

KPI?

Answers?

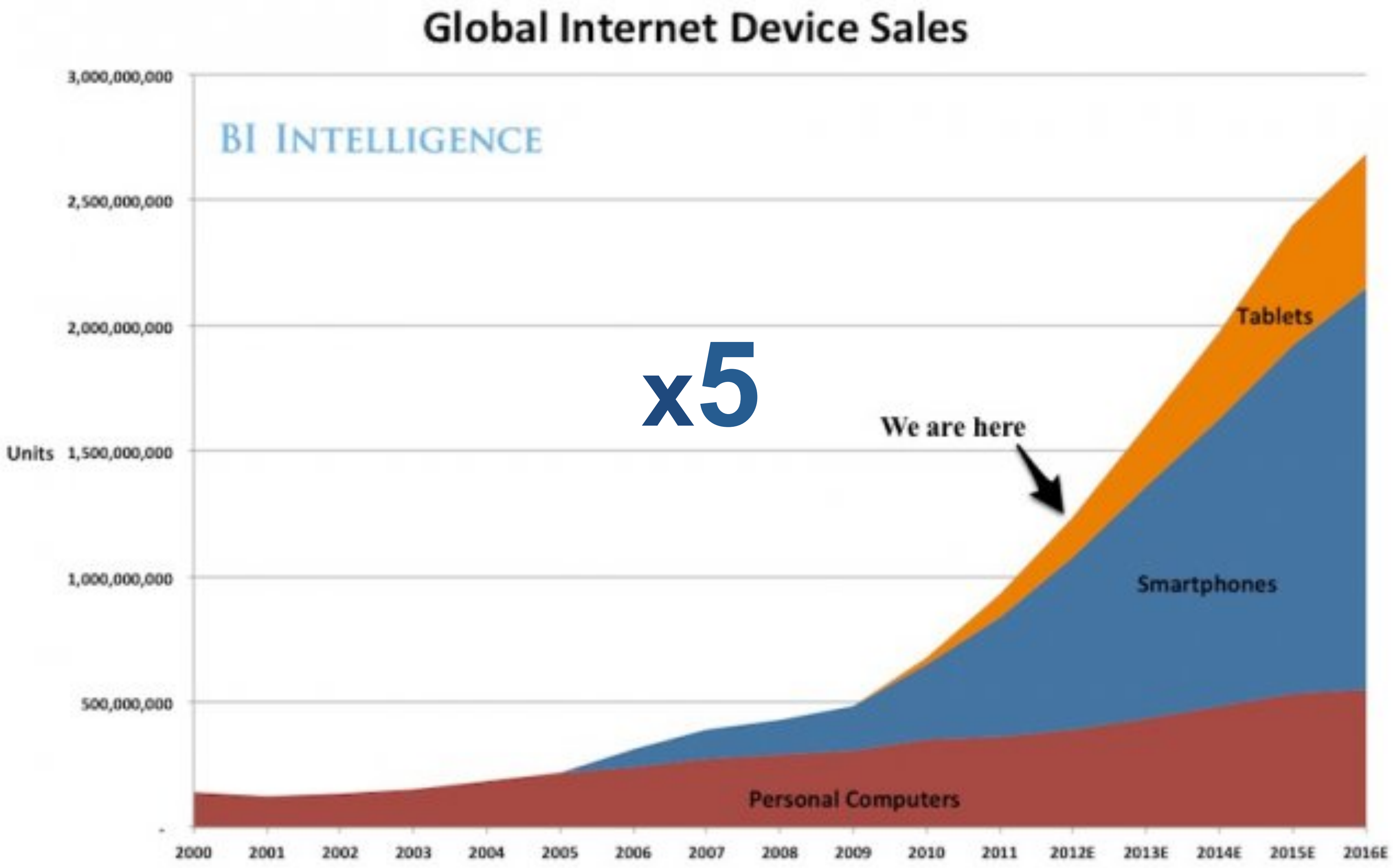
Security?

Cloud Computing
Market transformation

Cloud is NOT a technology is a market transformation

In 2020, people will interact each day with more than 70 devices connected to Internet. Nowadays we interact with less than 10 devices connected. The M2M phenomenom will boots Cloud and Internet users and bandwidth use. From 1 billion users today to 3 billion devices connected in 5 years

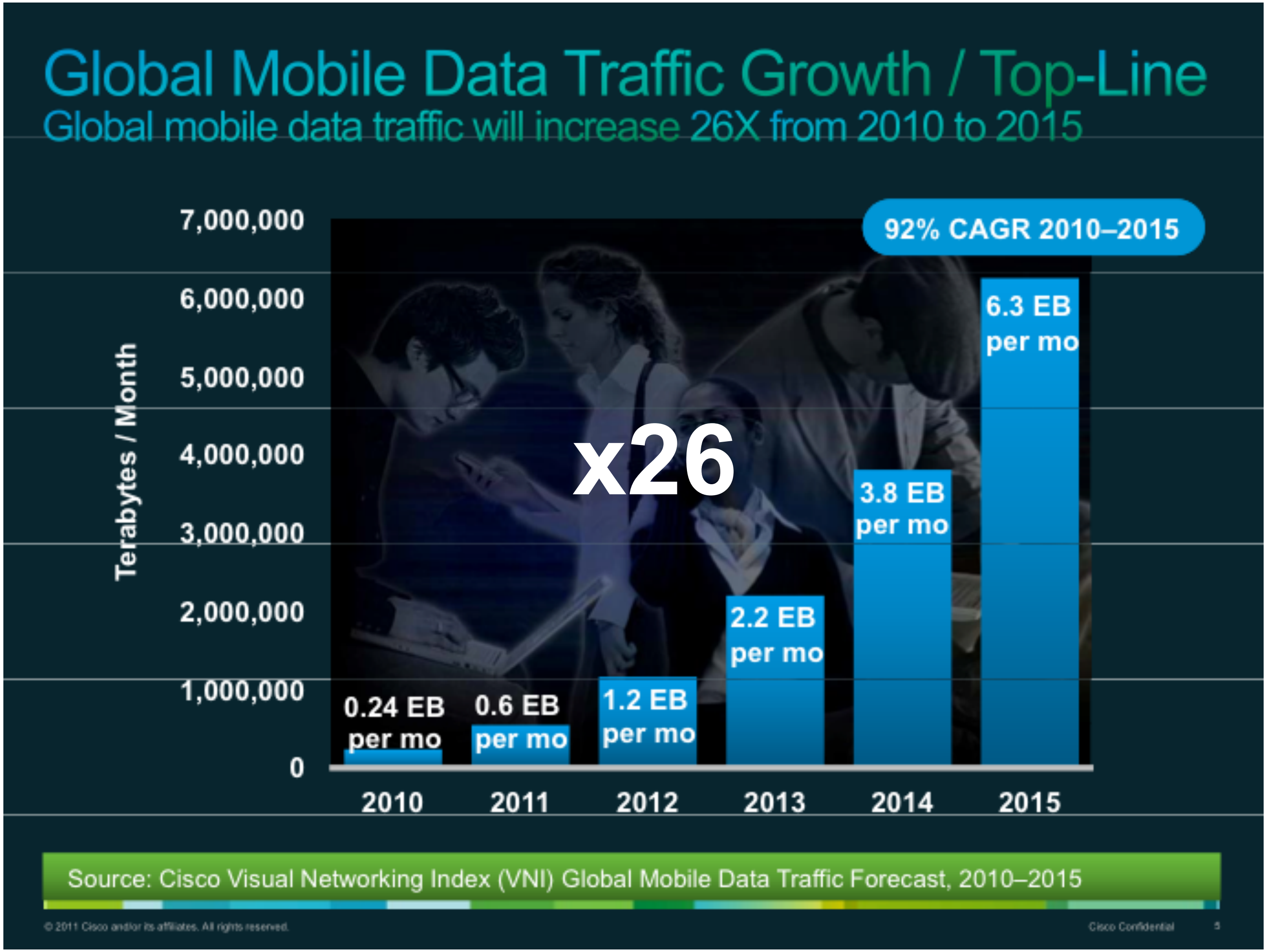
By 2014 will be more connected devices to Internet than people on Earth



x5

We are here

Source: Gartner, IDC, Strategy Analytics, company filings, BI Intelligence estimates



Global Mobile Data Traffic Growth / Top-Line

Global mobile data traffic will increase 26X from 2010 to 2015

Source: Cisco Visual Networking Index (VNI) Global Mobile Data Traffic Forecast, 2010–2015

Mobility as an answer for : Availability

TELEFONICA

Mercado: CONTINUO
Precio: 18,31
Fecha: 13/03 %: 1,16
Divisa: EUR Hora: 11:18
Volumen: 8.552.713,00
Max. Sesión:18,35
Mix. Sesión:17,80

Platforms?

Security?

BYOD?

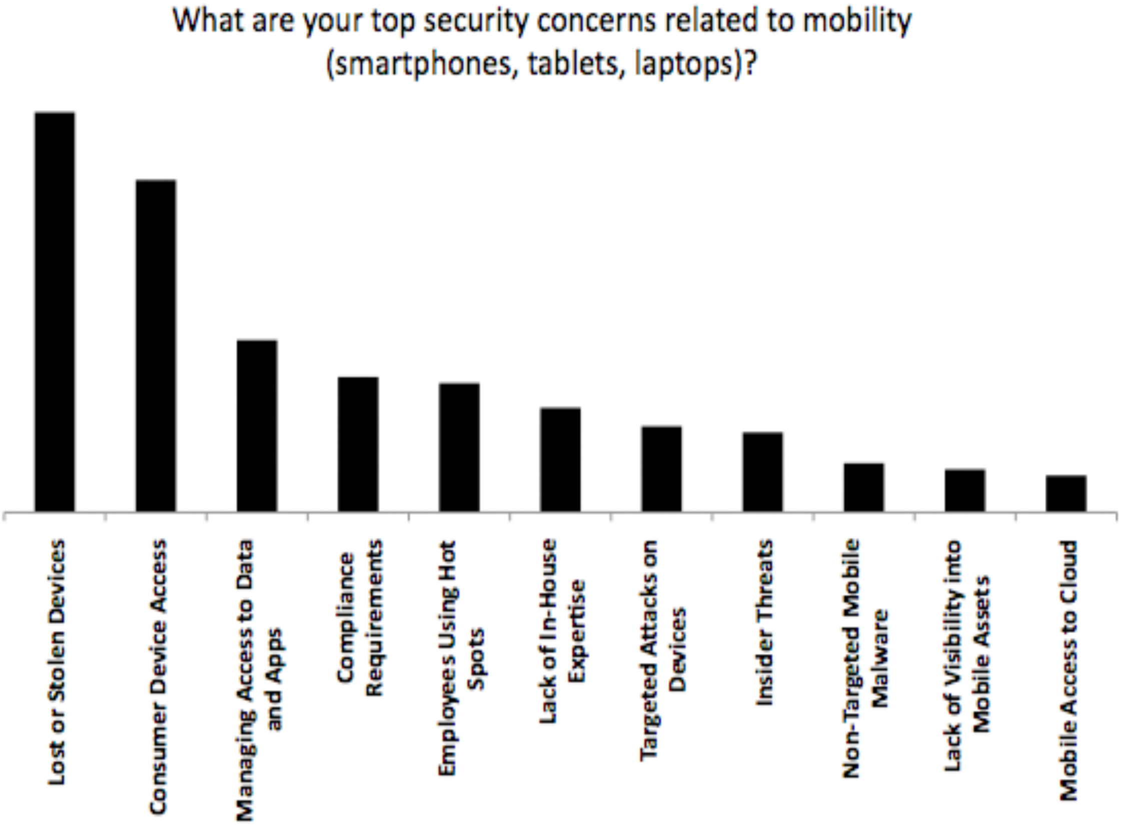
Applications?

Standards?

Backup?

Mobile Risk

Data protection and access top security concerns



http://searchmobilecomputing.techtarget.com/

BYOD `Bring Your Own Device´

BYOD and consumerization, is one based on the desire of employees to use their own mobile devices (phones, smartphones, tablets, laptops ...) in the workplace and access to information from this company, such as the corporate email, DB or file servers.

It is a reality accepted by IT departments, in the post-pc

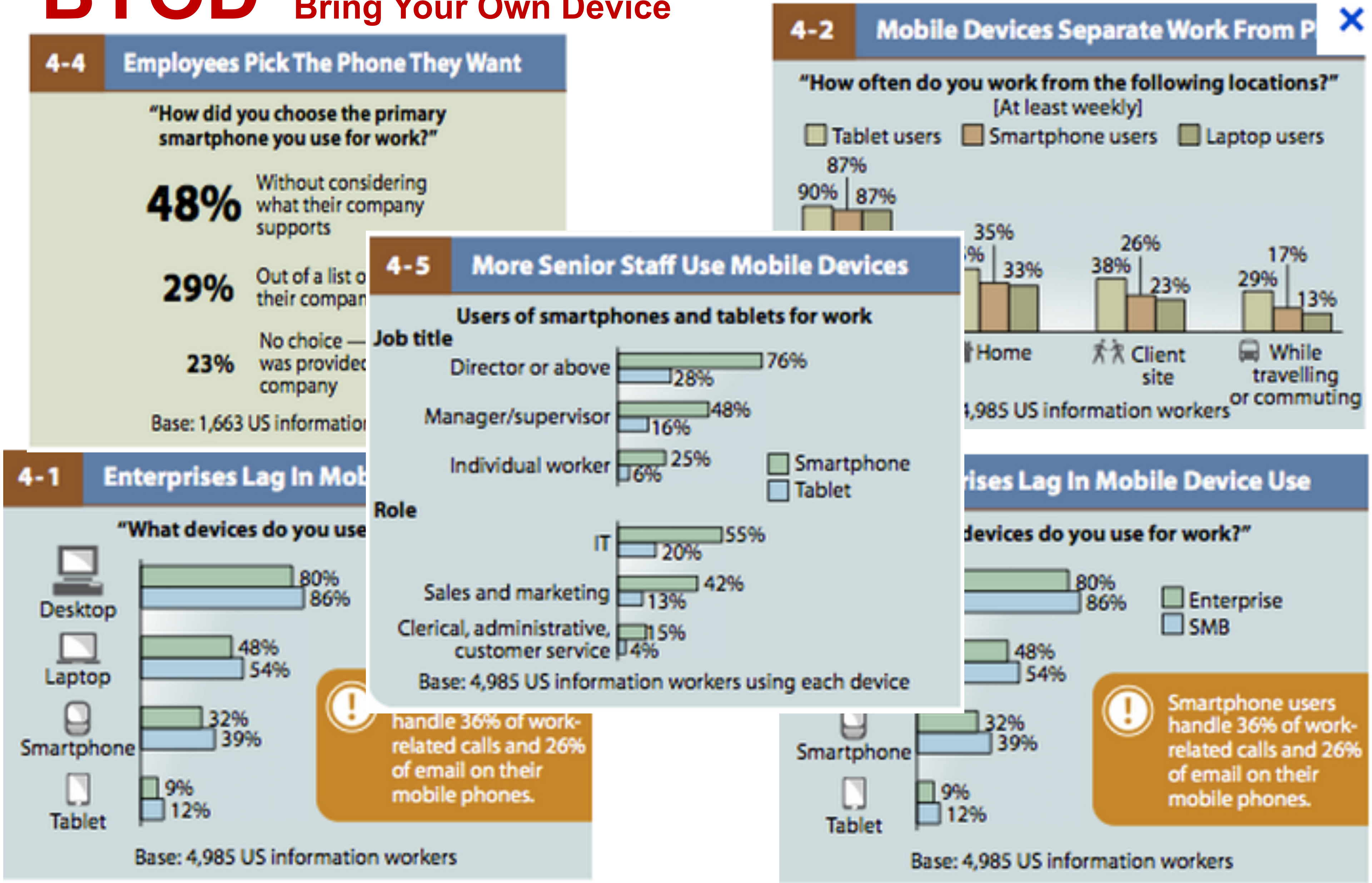
According to a survey of CISCO over 90% of CIOs surveyed said they permit, even doing the "blind eye," the use of mobile devices owned by employees to access their data.

Of the principals surveyed more than two thirds have overcome fears this trend and see it as something positive for the organization.

Yet another study, this time from the company BT, puts out the lack of vision of the potential risks of this practice on the part of employees, as only one in four sees risk in using their own devices, when almost 40% of companies have experienced security incidents related to this issue.

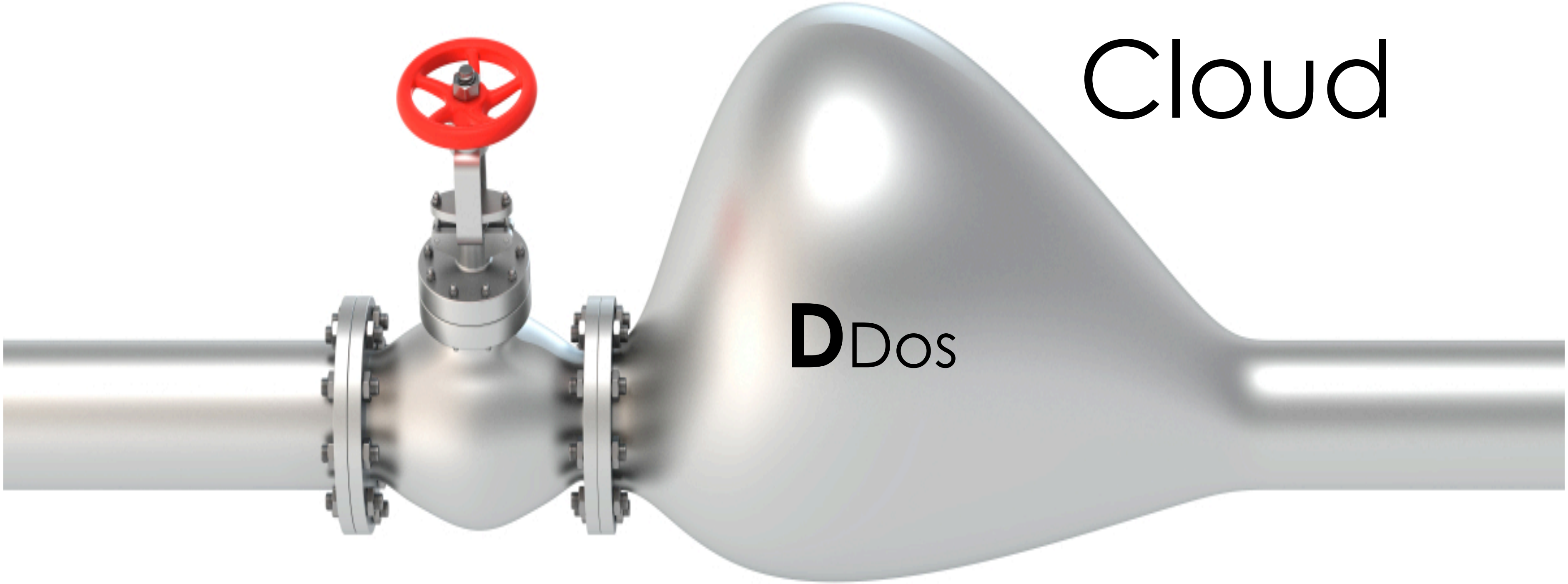
BYOD the New Threat door

BYOD `Bring Your Own Device´



More Users + More Devices + More Services

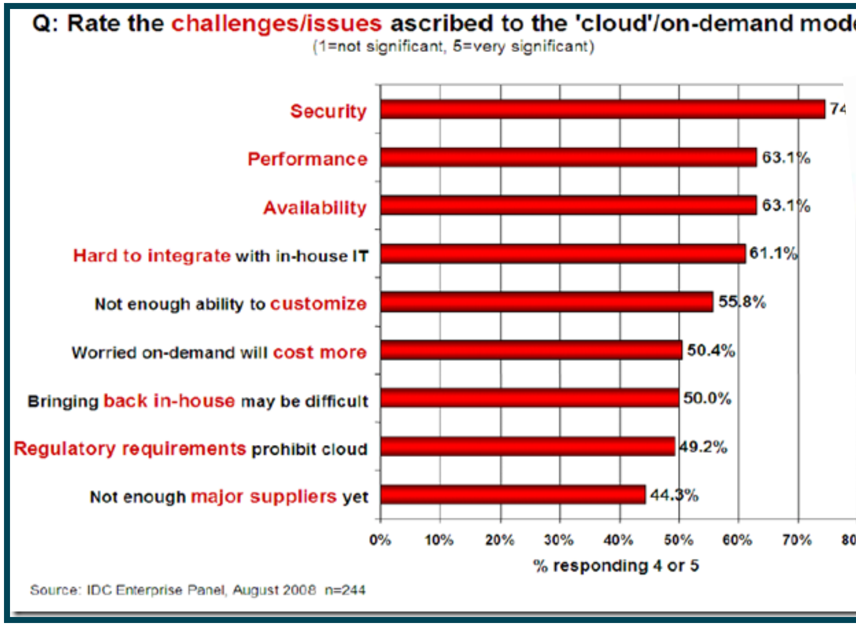
Mobile+ Cloud



DDos

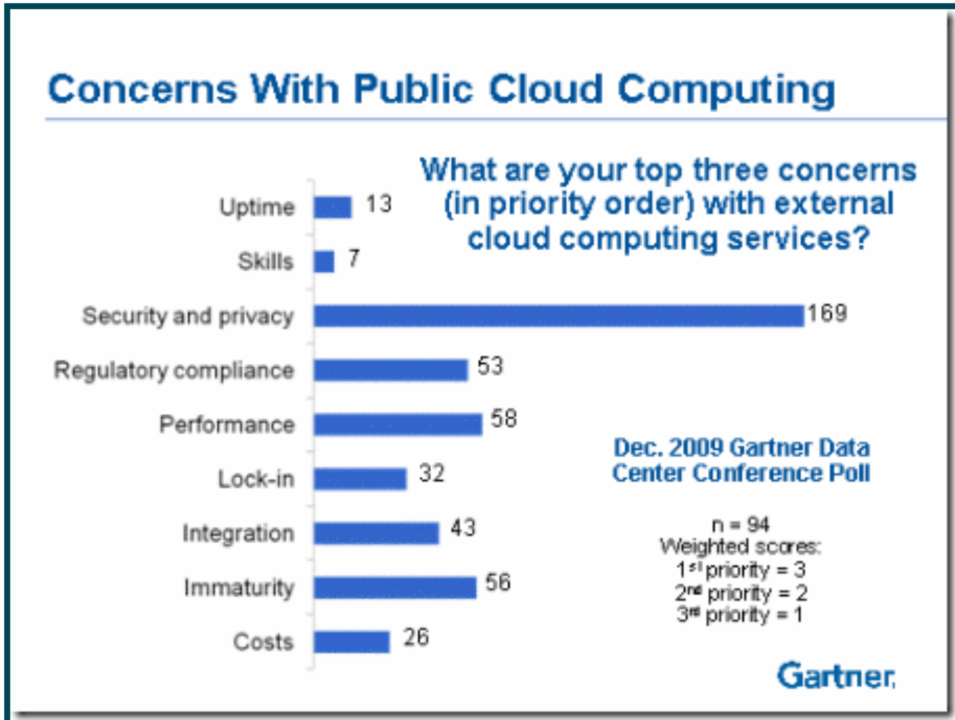
Reduced Stress =**More** Capacity + **More** Control + **More** Visibility

Concerns about Public Cloud (not private Cloud?)


Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)

Source: IDC Enterprise Panel, August 2008 n=244

CLOUD Security concerns


Concerns With Public Cloud Computing

What are your top three concerns (in priority order) with external cloud computing services?

Dec. 2009 Gartner Data Center Conference Poll

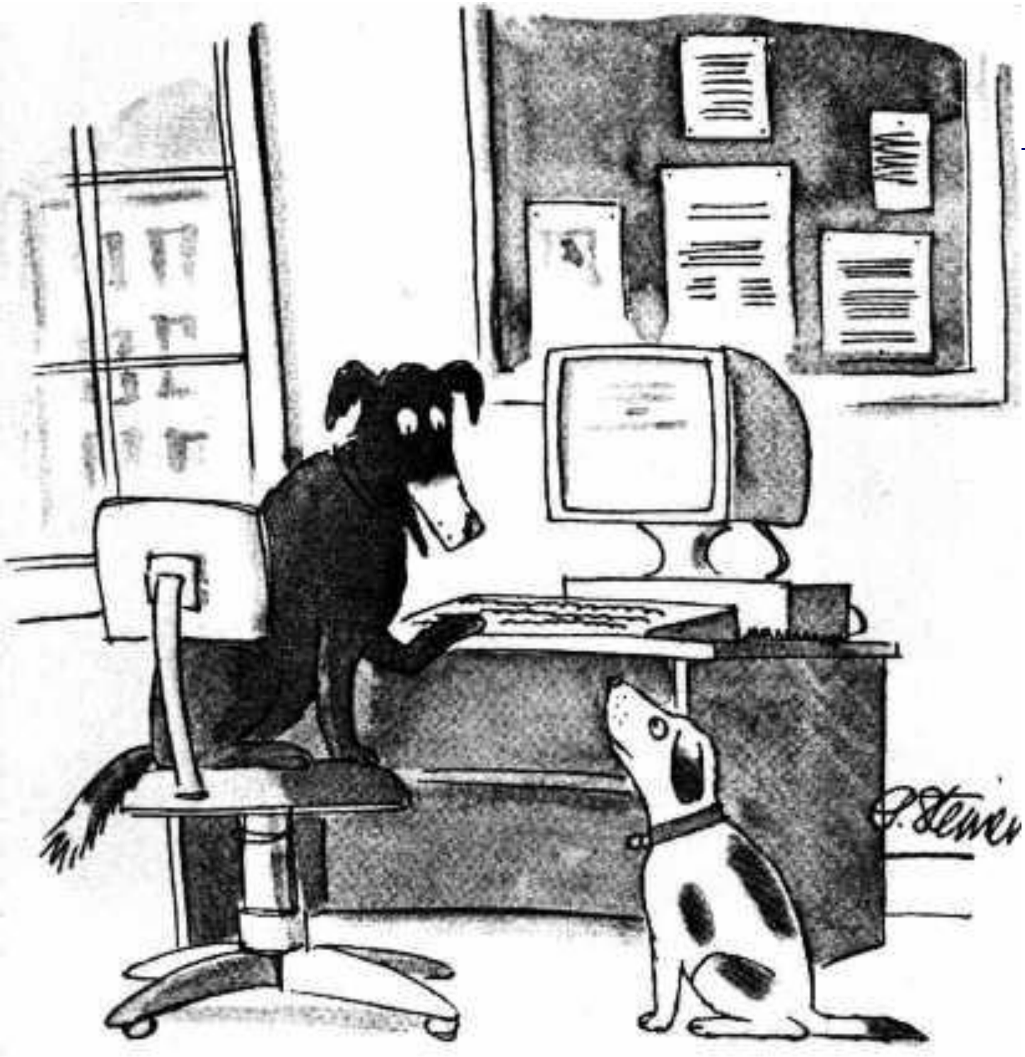
n = 94
Weighted scores:
1st priority = 3
2nd priority = 2
3rd priority = 1

Gartner.

What Control Mechanisms Does the Vendor Provide?

- Identity and access management
  - Federation, strong authentication, access and roles
  - How to verify who has access to what and who has done what?
- Data confidentiality protection
  - Encryption of data at rest and in transit
  - How do you manage encryption keys?
- Monitoring and alerting
  - DLP, IPS, SoD, DAM
  - How do you perform an audit?
- Discovery and investigation
  - How do you do forensics in multiple jurisdictions?
  - What is a business record?
  - Don't forget law enforcement access

If they don't build it in, you can't use it.



"On the Internet, nobody knows you're a dog."

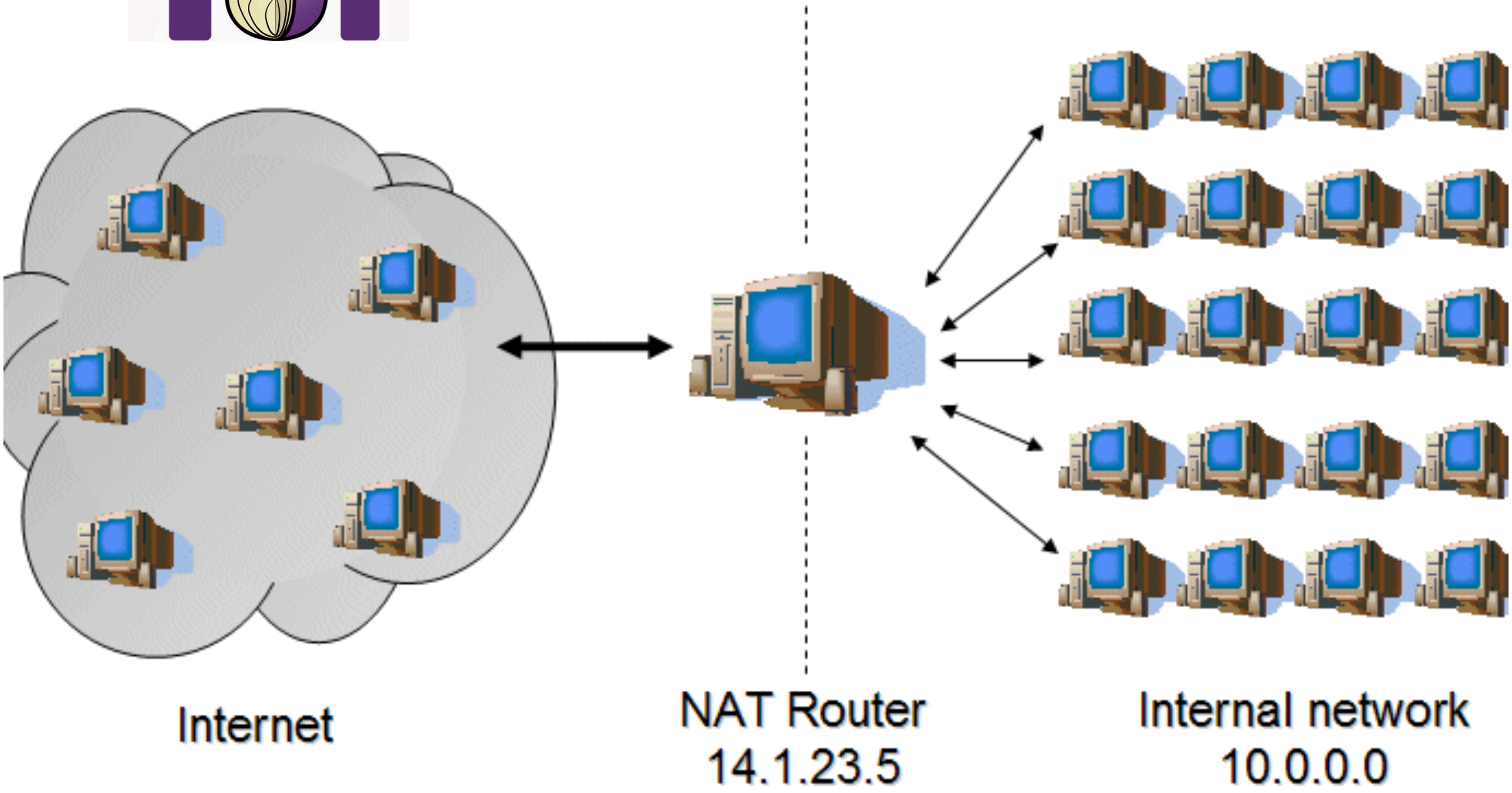
IDENTITY?

July,5th 1993.THE NEWYORKER

WE ARE ANONYMOUS

Because none of us are as cruel as all of us.

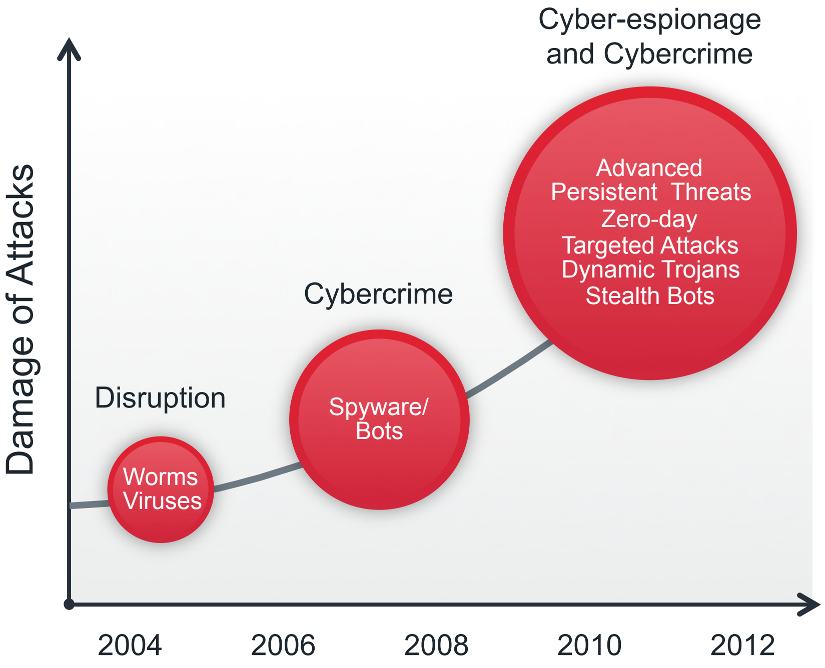
Why is this happening? IPv4



Why is this happening? IPv4

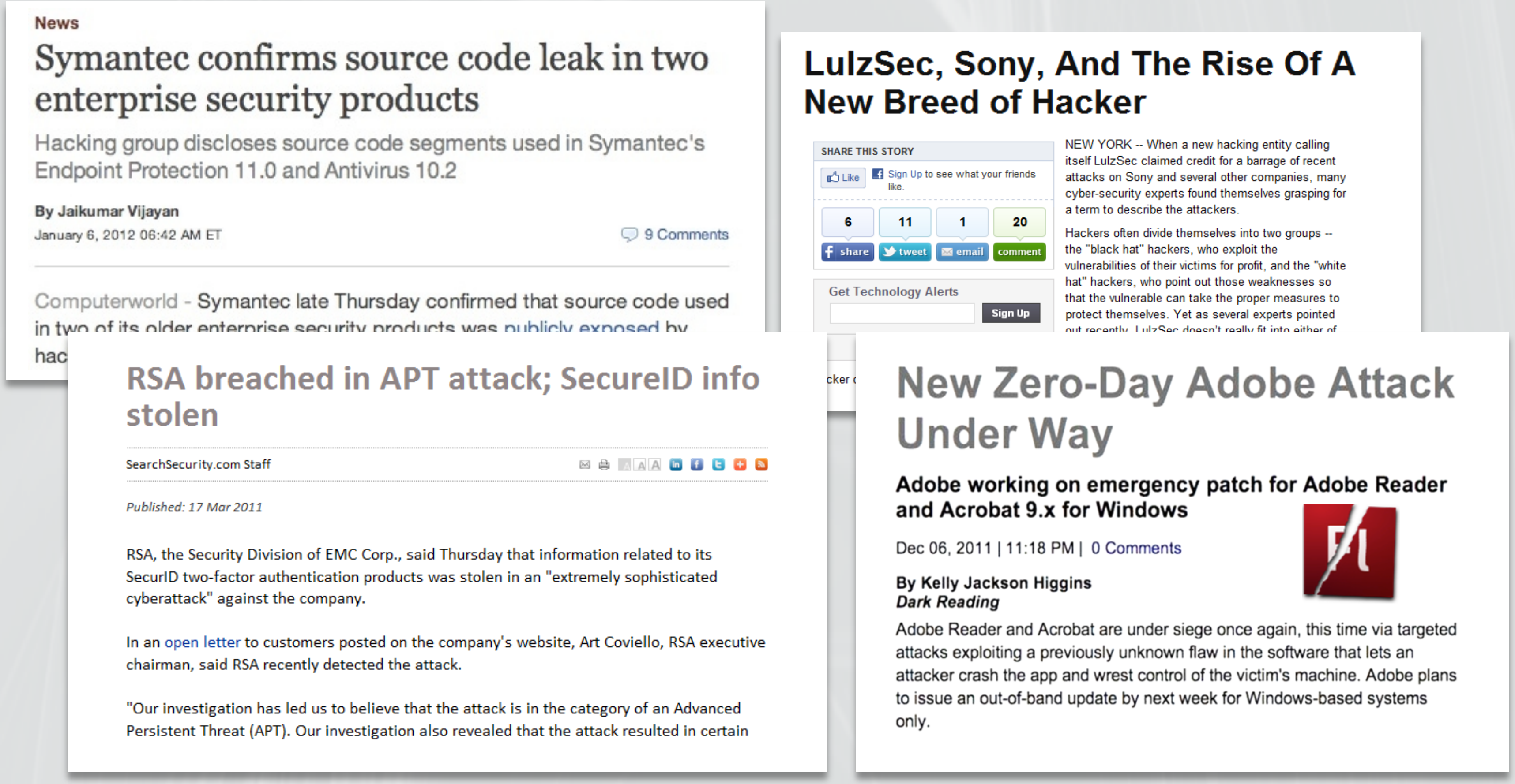
Growing of new attacks and APTs

- Number of threaths **x5** in 4 years
- Nature of threats and attacks change:
  - From general and diverse to persistent, avanced and oriented
- Avanced attacks grow
  - High victims level profile (i.e, RSA; Symantec, Google)
  - Great variety of new APTs like Aurora Operation, Shady RAT, GhostNet, Night Dragon, Nitro



> **“Organizations face an evolving threat scenario that they are ill-prepared to deal with….advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems.”**
>
> Gartner, 2012

APT Attacks. Attacks profile has increased



News

Symantec confirms source code leak in two enterprise security products

Hacking group discloses source code segments used in Symantec's Endpoint Protection 11.0 and Antivirus 10.2

By Jaikumar Vijayan

January 6, 2012 06:42 AM ET

9 Comments

Computerworld - Symantec late Thursday confirmed that source code used in two of its older enterprise security products was publicly exposed by hac

LulzSec, Sony, And The Rise Of A New Breed of Hacker

NEW YORK -- When a new hacking entity calling itself LulzSec claimed credit for a barrage of recent attacks on Sony and several other companies, many cyber-security experts found themselves grasping for a term to describe the attackers.

Hackers often divide themselves into two groups -- the "black hat" hackers, who exploit the vulnerabilities of their victims for profit, and the "white hat" hackers, who point out those weaknesses so that the vulnerable can take the proper measures to protect themselves. Yet as several experts pointed out recently, LulzSec doesn't really fit into either of

cker c

RSA breached in APT attack; SecureID info stolen

SearchSecurity.com Staff

Published: 17 Mar 2011

RSA, the Security Division of EMC Corp., said Thursday that information related to its SecurID two-factor authentication products was stolen in an "extremely sophisticated cyberattack" against the company.

In an open letter to customers posted on the company's website, Art Coviello, RSA executive chairman, said RSA recently detected the attack.

"Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain

New Zero-Day Adobe Attack Under Way

Adobe working on emergency patch for Adobe Reader and Acrobat 9.x for Windows

Dec 06, 2011 | 11:18 PM | 0 Comments

By Kelly Jackson Higgins
Dark Reading

Adobe Reader and Acrobat are under siege once again, this time via targeted attacks exploiting a previously unknown flaw in the software that lets an attacker crash the app and wrest control of the victim's machine. Adobe plans to issue an out-of-band update by next week for Windows-based systems only.

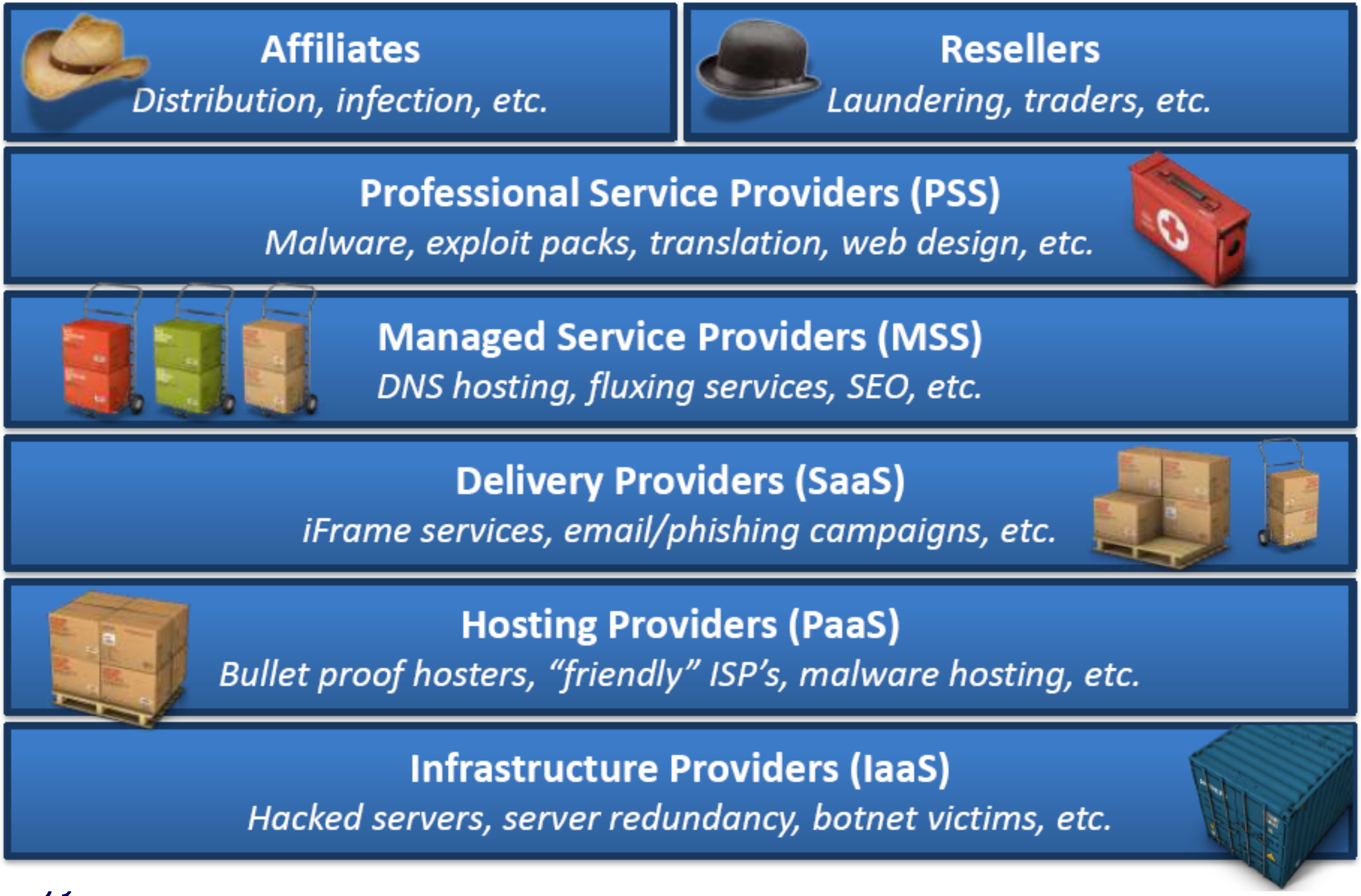
APTs, new tools for DDoS / TDoS

Advanced Persistent Threats (APTs) are created by different organizations from hackers like Lulzsec, Anonymous,etc. Also by Federeal Goverments like CIA, Mossad, etc.Their main motivation are:

1. **Goverment**
2. **Economical**
3. **Technical**
4. **Military**

Botnets

Botnet Ecosystem



Affiliates

Distribution, infection, etc.

Resellers

Laundering, traders, etc.

Professional Service Providers (PSS)

Malware, exploit packs, translation, web design, etc.

Managed Service Providers (MSS)

DNS hosting, fluxing services, SEO, etc.

Delivery Providers (SaaS)

iFrame services, email/phishing campaigns, etc.

Hosting Providers (PaaS)

Bullet proof hosters, "friendly" ISP's, malware hosting, etc.

Infrastructure Providers (IaaS)

Hacked servers, server redundancy, botnet victims, etc.

Botnets

The Criminal Operations Team

Malware Author(s)

- Original malware creator(s)
- Offer malware “off-the-rack” or custom built
- May offer DIY construction kits
- Money-back guarantee if detected
- 24x7 support

Botnet Master

- Individual or criminal team that owns the botnet
- Maintains and controls the botnet
- Holds admin credentials for CnC

Botnet Operator

- Operates a section of the botnet for direct financial gain
- Issues commands to the bot agents
- May be the Botnet Master

Distribution Provider (MSP)

- Specialized distribution network
- Attracts and infects victims
- Global & targeted content delivery
- Delivery through Spam/drive-by/USB/etc.
- Offers 24x7 support

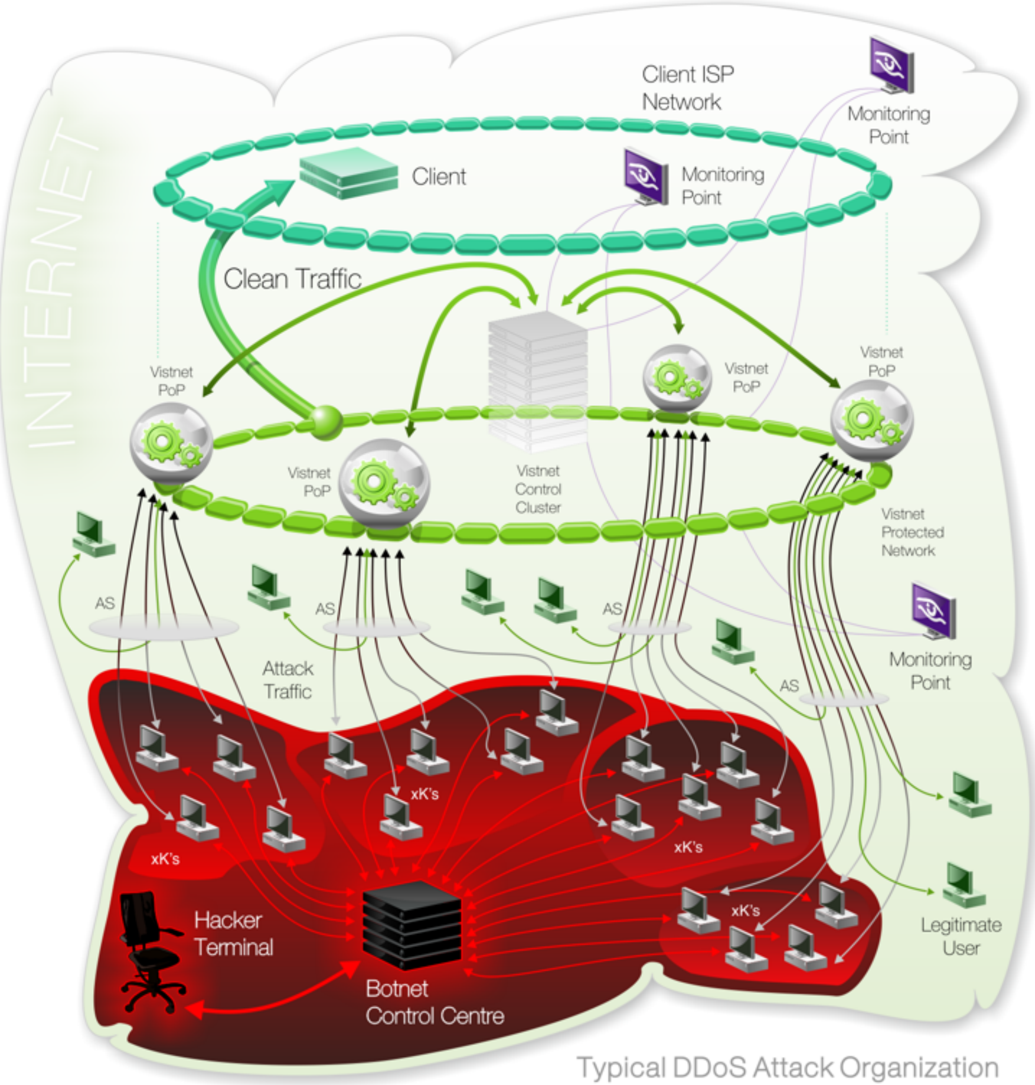
Resilience Provider (MSP)

- Provides CnC resilience services
- Anti-takedown network construction
- Bullet-proof domain hosting
- Fast-flux DNS services
- Offers 24x7 Support

Hacking Ecosystem

- Each piece of information, each tool, and every vector has a price.

DDoS the increasing threat, for all Internet Services



Typical DDoS Attack Organization

Reason 1
- Universal

Reason 2
- Cheap

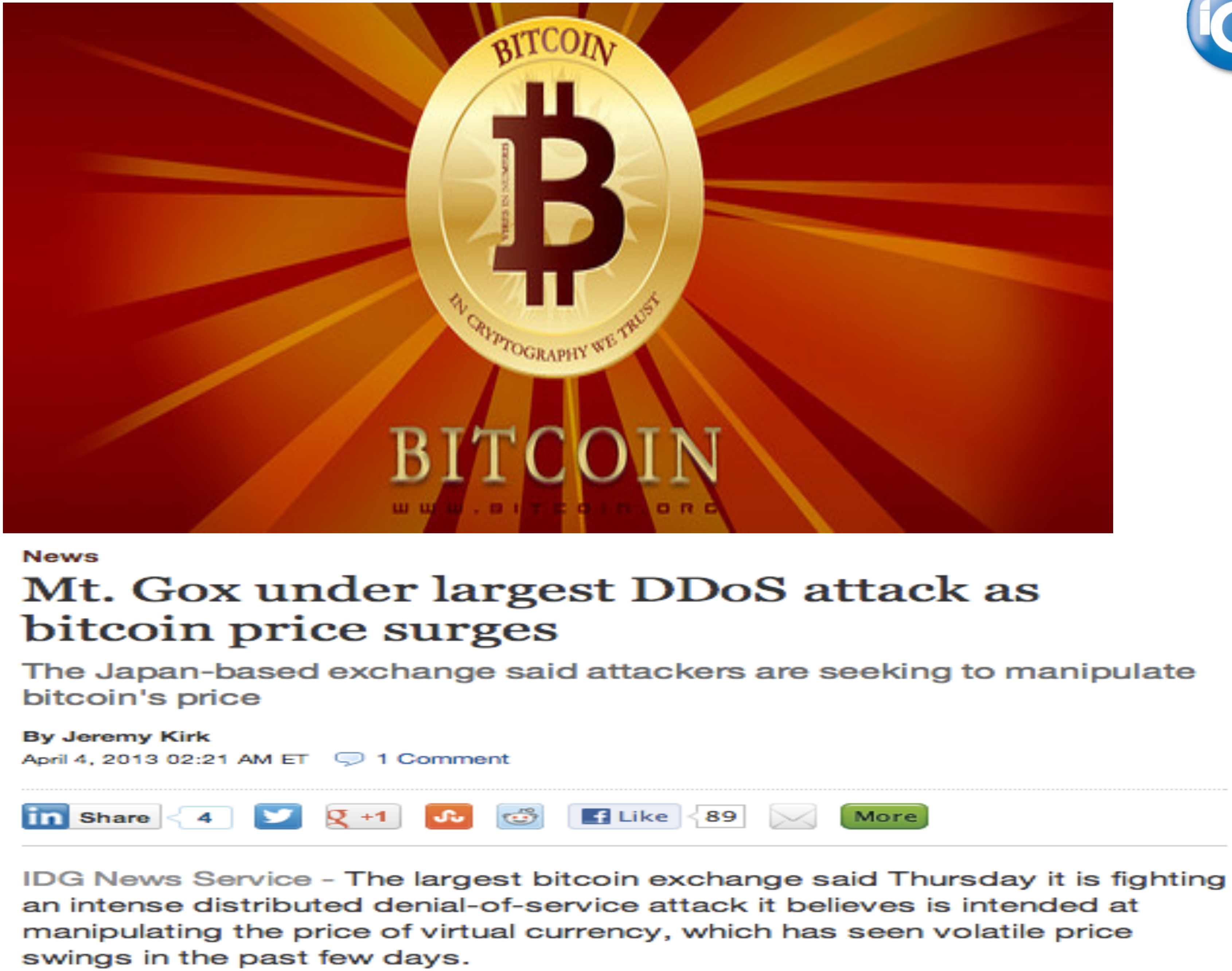
Reason 3
- Eficiency

Reason 4
- No pushment

Reason 5
- Big Impact

Reason 6
- Easy to replicate

Reason 7
- Underestimate



News

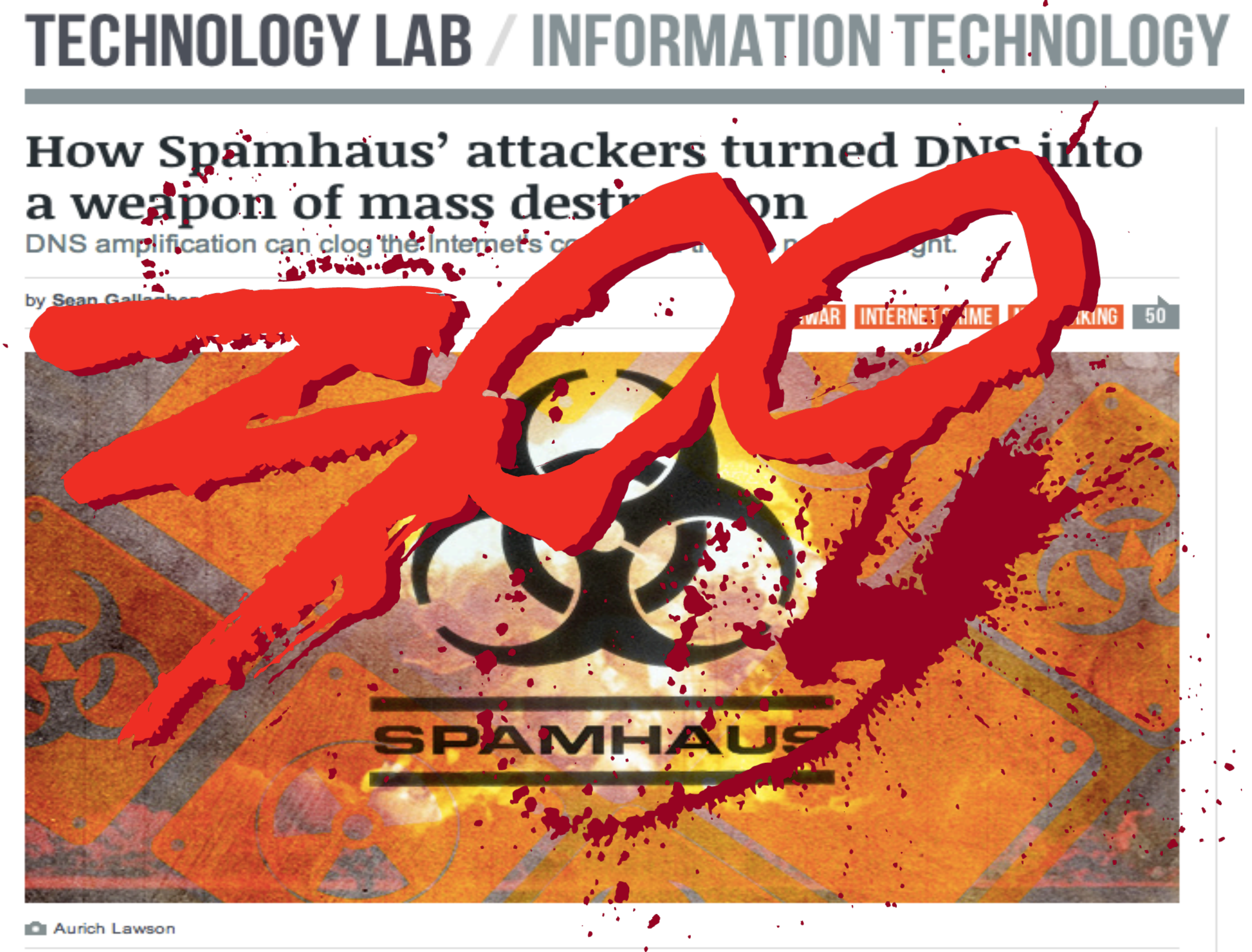
Mt. Gox under largest DDoS attack as bitcoin price surges

The Japan-based exchange said attackers are seeking to manipulate bitcoin's price

By Jeremy Kirk

April 4, 2013 02:21 AM ET 1 Comment

IDG News Service - The largest bitcoin exchange said Thursday it is fighting an intense distributed denial-of-service attack it believes is intended at manipulating the price of virtual currency, which has seen volatile price swings in the past few days.



TECHNOLOGY LAB / INFORMATION TECHNOLOGY

How Spamhaus’ attackers turned DNS into a weapon of mass destr on

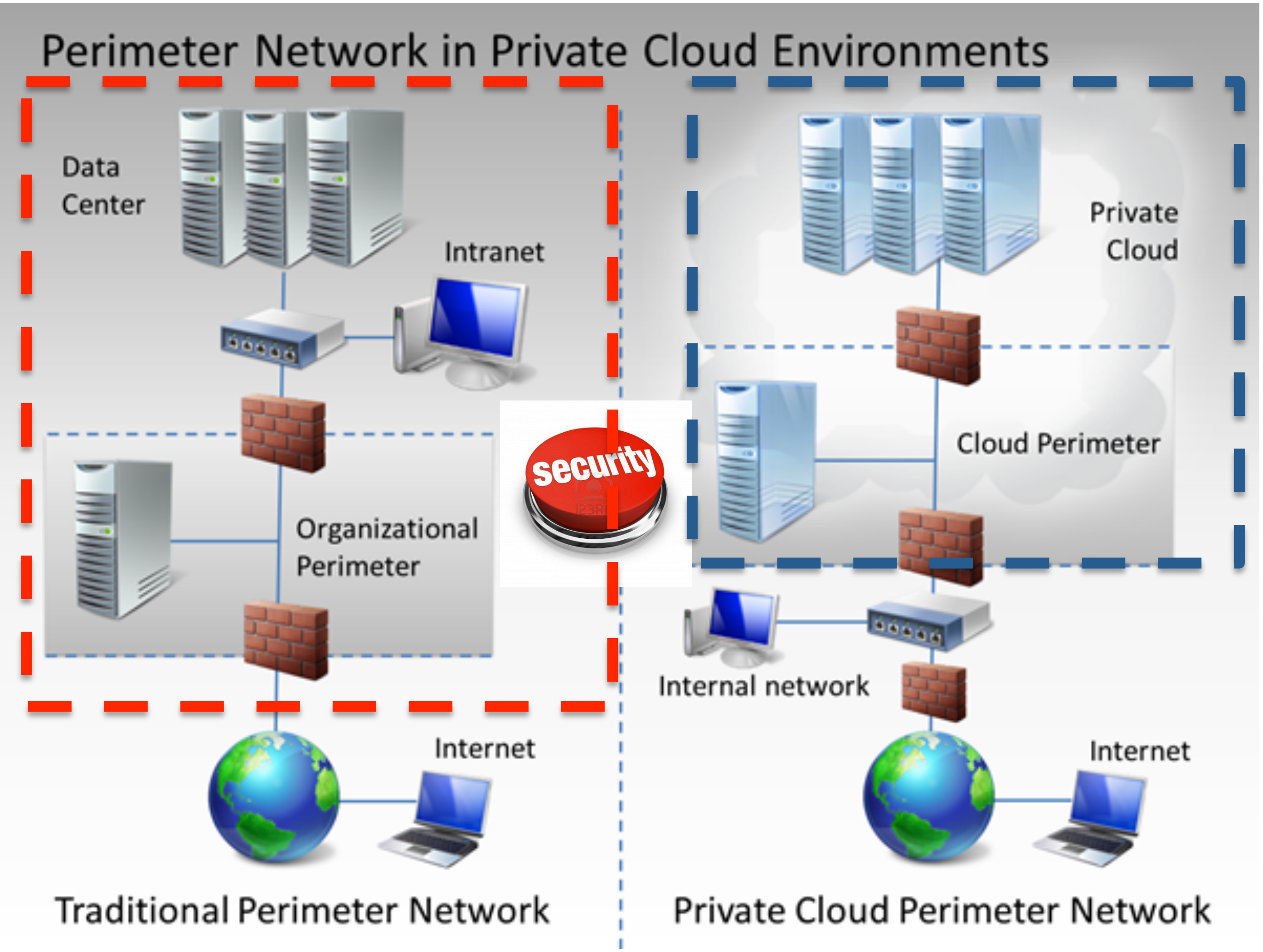
DNS amplification can clog the Internet's co ght.

by Sean Gallagher

WAR INTERNET CRIME KING 50

Aurich Lawson

The New Perimeter. Security for and from Cloud.

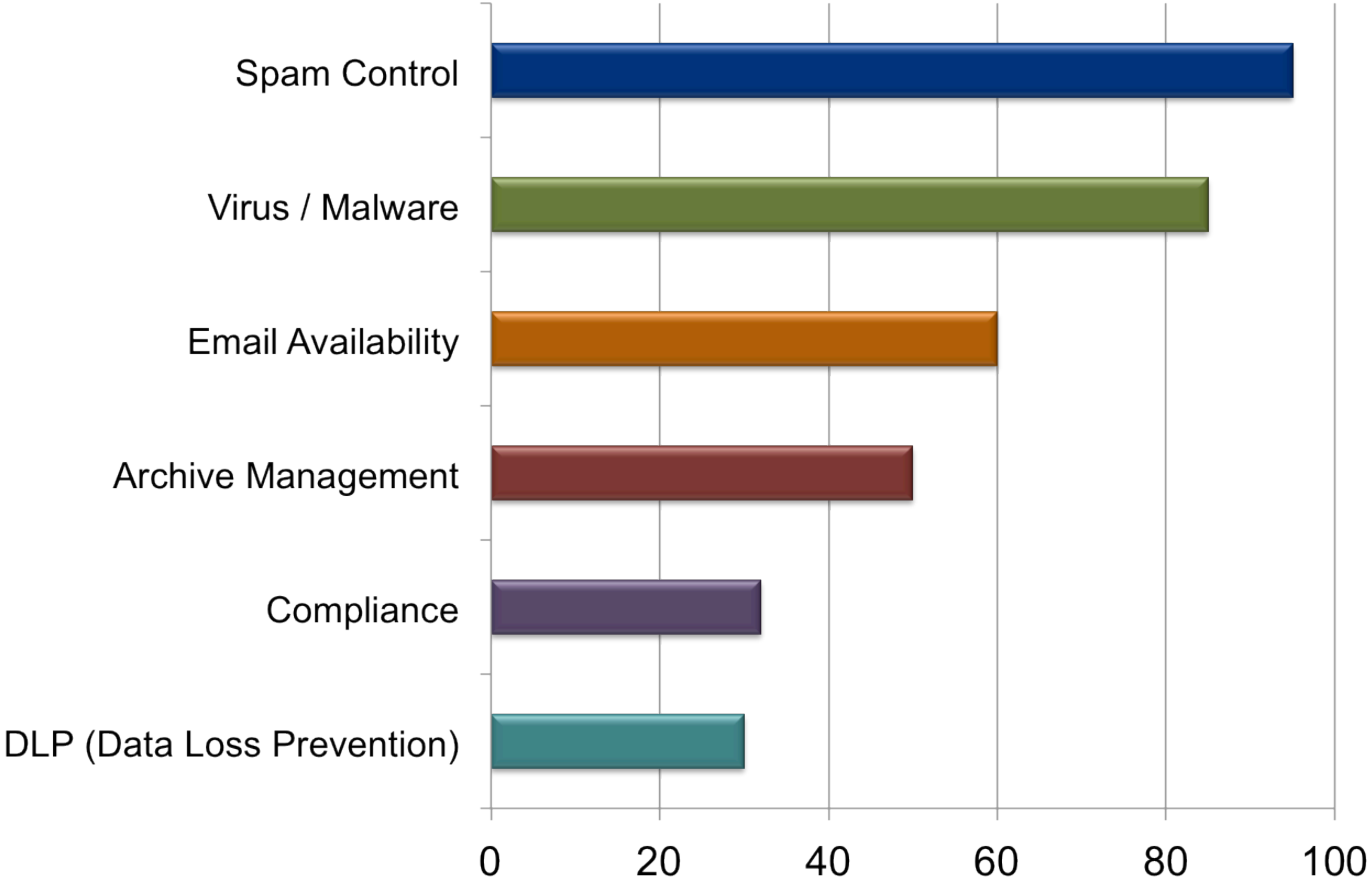


- Cloud must play an active defense role
- Cloud must be an active player for the perimeter defense
- Cloud can be use nowadays as an active extension of our security perimeter
- Cloud nowadays is able to provide at least secure email and internet access
- Cloud must provide active defense

ACT don't REACT

Email Security

Security Challenges of Email in the Cloud



Conclusion: Secure Cloud+ Mobile

Clean Pipes

AntiDDoS

NAT

DNS

ID Mgmt

AntiAPTs

DPI

WAF

DataCentre

SOC

LTE

IPv6

Juan Miguel Velasco López-Urda
jmvelasco@aiuken.com
CEO Aiuken Solutions

You will never reach
your destination
if you stop and throw
stones at every dog
that barks.

- Winston Churchill