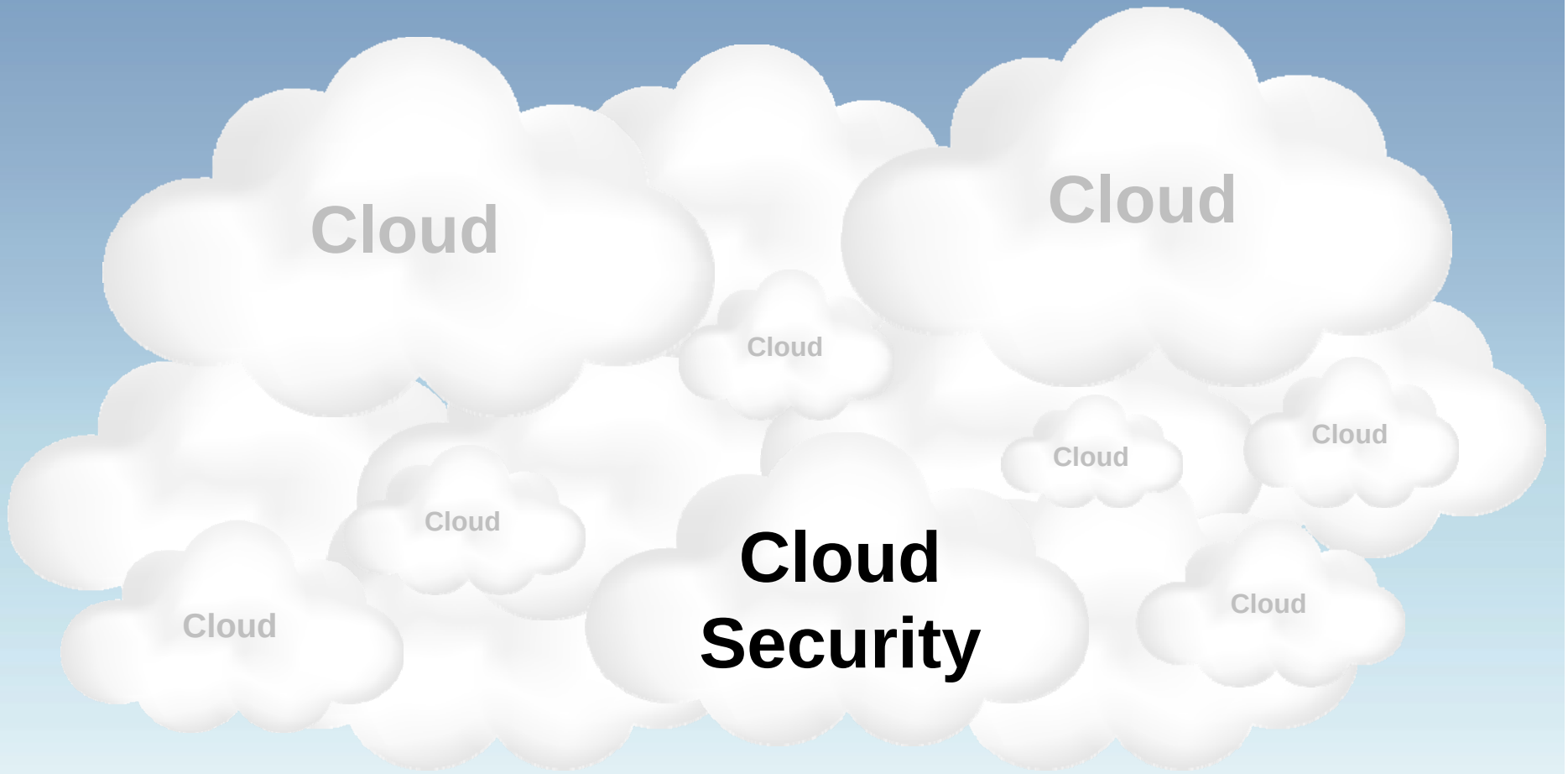


Billy Chuang

Presales Consultant Manager

F5 Networks

Platform as a Service

Grid Computing

Software as a Service

Dynamic Computing Infrastructure

Public Cloud

Framework Computing

Elastic Compute Environment

Dynamic Connectivity Intelligence

Utility Computing

DYNAMIC PROVISIONING

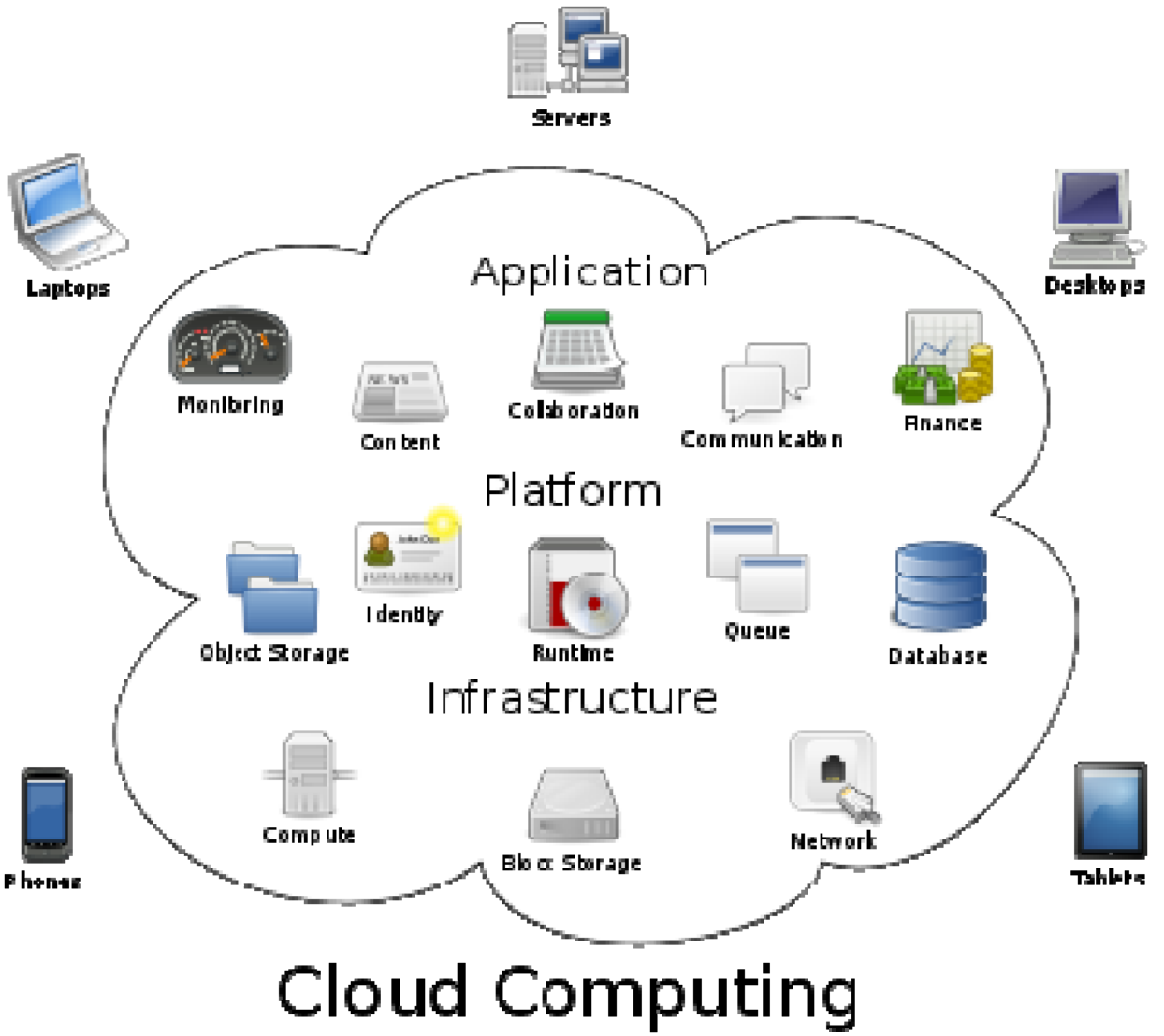
Private Cloud

Infrastructure as a Service

RESOURCES AS A SERVICE

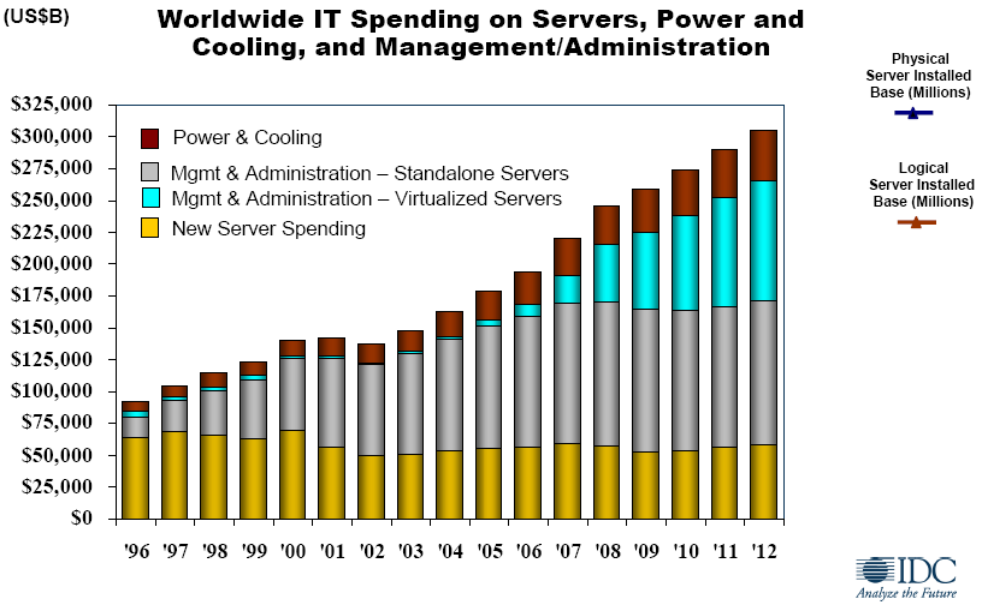
Unified Computing System

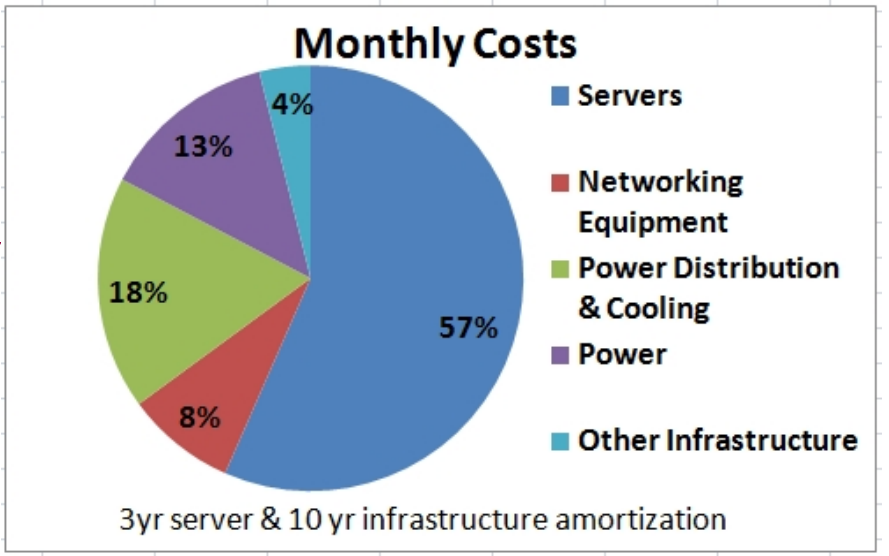
What is Cloud ?



Data Center

- Power/Cooling
- Cost Control
- Fewer Sites
- Improved Design
- Virtualization





Global CIO Strategies Focus on Creating New Infrastructures for Growth and Efficiency

	2011	2010	2009	2008
Developing or managing a flexible infrastructure	**1**	**8**	**11**	**11**
Delivering applications and growth projects	2	1	3	1
Reducing the cost of IT	3	3	2	10
Improving IT management and governance	4	6	4	7
Consolidating IT operations and resources	5	9	9	12
Reorganizing IT (attracting/retaining IT personnel)	6	10	8	3
Expanding the use of information/intelligence	7	7	10	9
Implementing business process improvements	8	4	5	6
Implementing cloud solutions (SaaS, PaaS, IaaS)	9	*	*	*
Improving/linking the business-IT relationship	10	2	1	2

* New response category

Gartner
Neil Rickard
Research Vice President - EMEA

What is Cloud and Why does it matter?

Mainframe

+ Centralized mgmt
+ Secure
- Limited access
- Inflexible
- Costly

Client/Server

+ Distributed CPU utilization
+ Added flexibility
- Complex / costly to deploy & manage
- Not secure
- Not efficient

Web

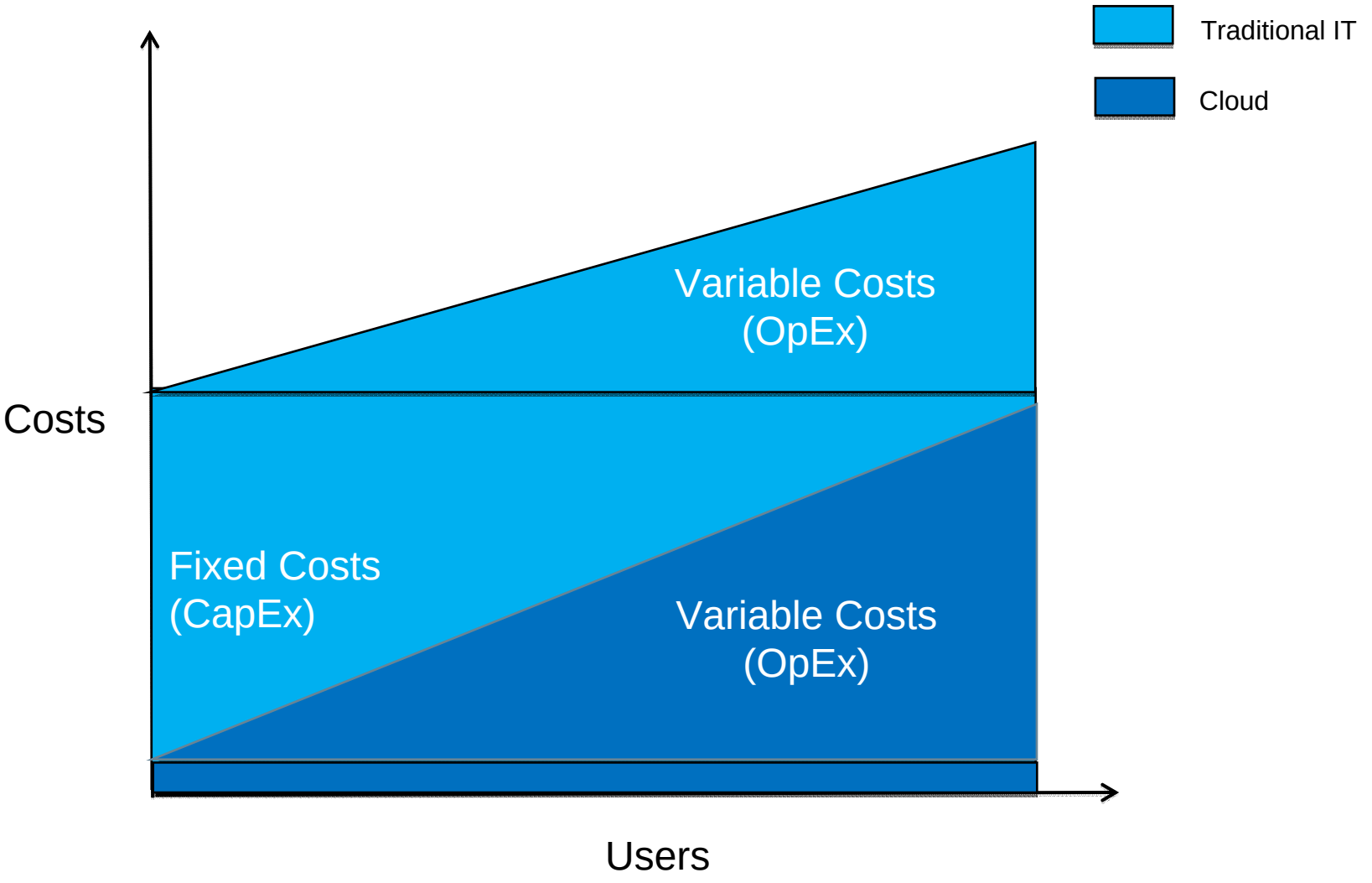
+ Simple to deploy and manage
+ Broader access
+ Scale
- Limited flexibility
- Limited efficiency
- Not secure

"Cloud"

+ Frictionless deployment
+ Simplified mgmt thru abstraction
+ On-demand scale
+ Unparalleled flexibility
+ Secure
+ Highly efficient
+ Data Center as a Service

Cloud is not hype - It's about Simplicity, Agility and most importantly, it's about Economics.

Traditional IT vs Cloud (Shared Infrastructure) It's all in the Economics



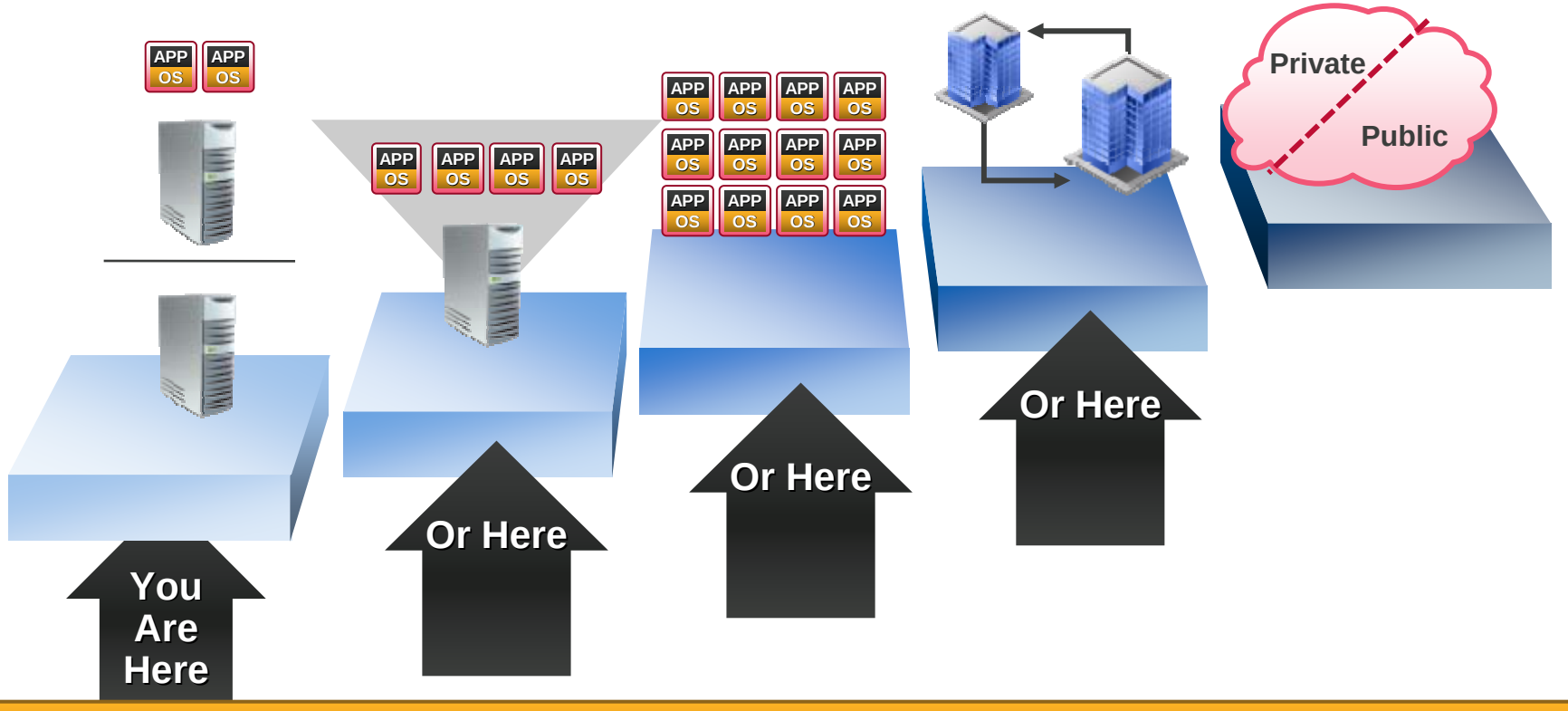
How does Cloud Computing differ from Virtualization?

Virtualization: The ability for a single device to look or act like many

Cloud Computing: The ability for a group of devices to provide dynamic, automated scalability

Dynamic Data Center Model

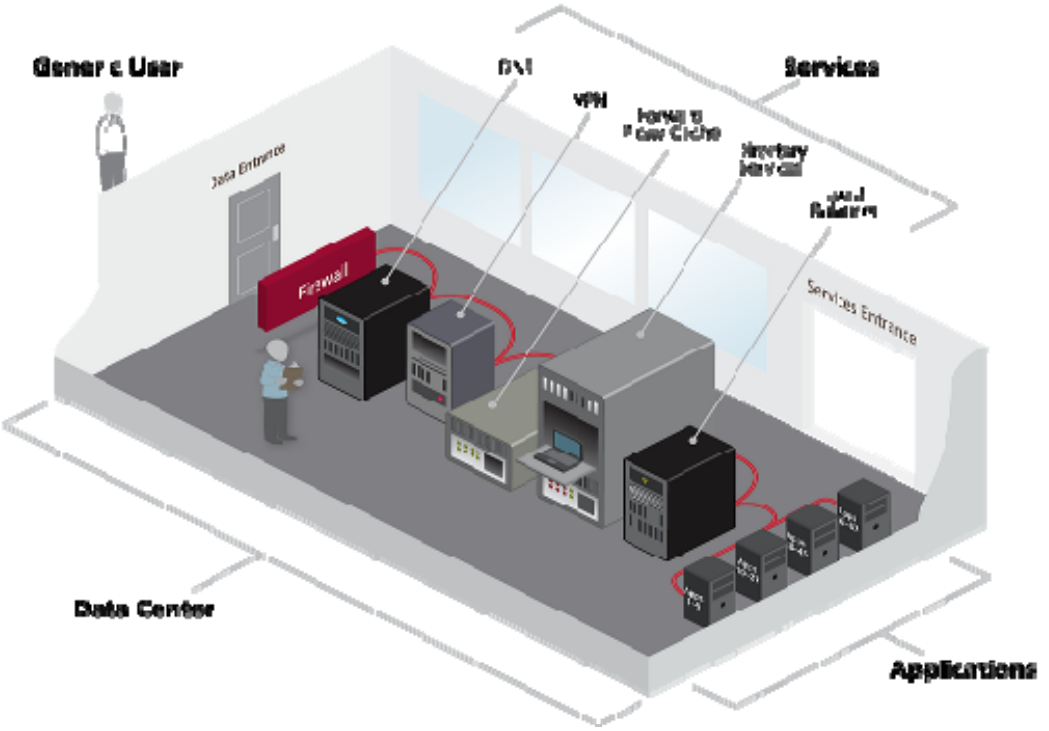
Separate	Consolidate	Aggregate	Automate	Liberate
Test and Development	Server Consolidation	Capacity On Demand	Self-Managing Datacenters	Enterprise Computing Clouds On and Off Premise



Enterprise Objective: An IT Services On-Demand Platform

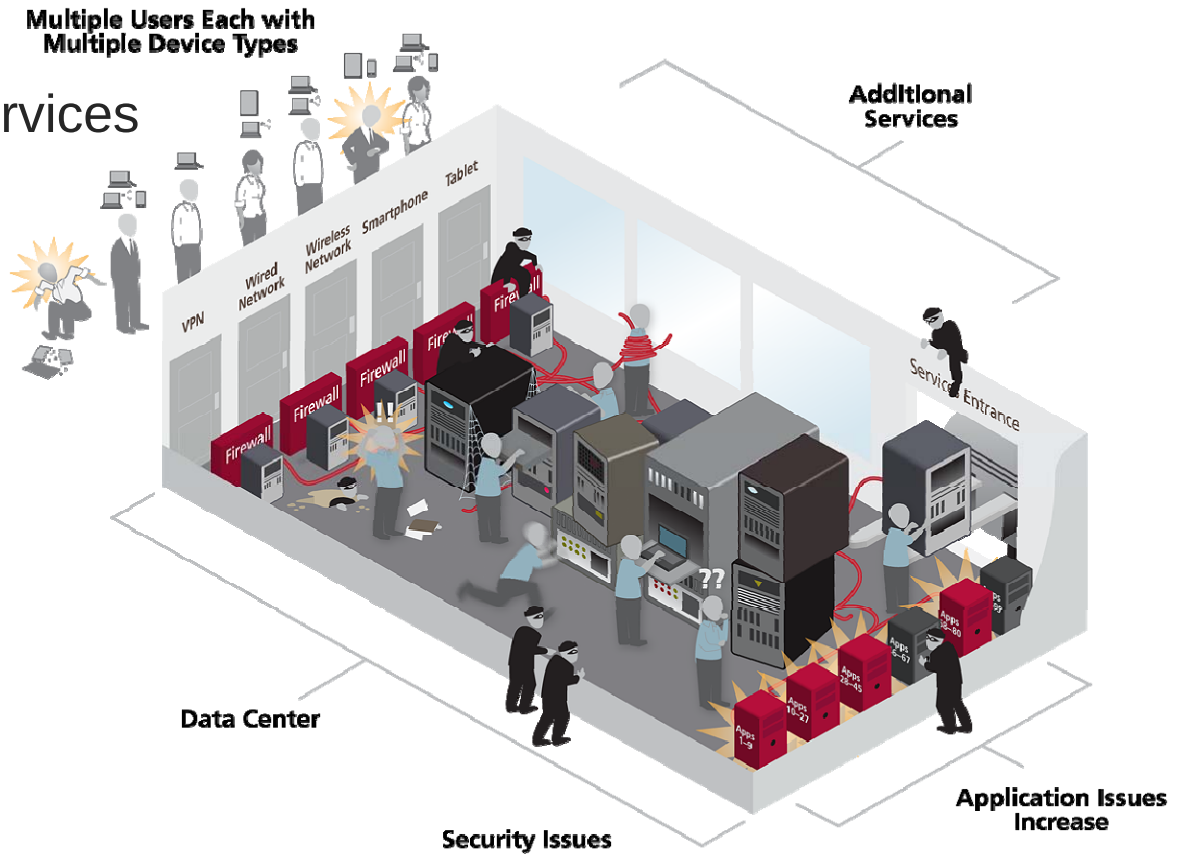
How the Static Data Center Falls Short

- It started simple



How the Static Data Center Falls Short

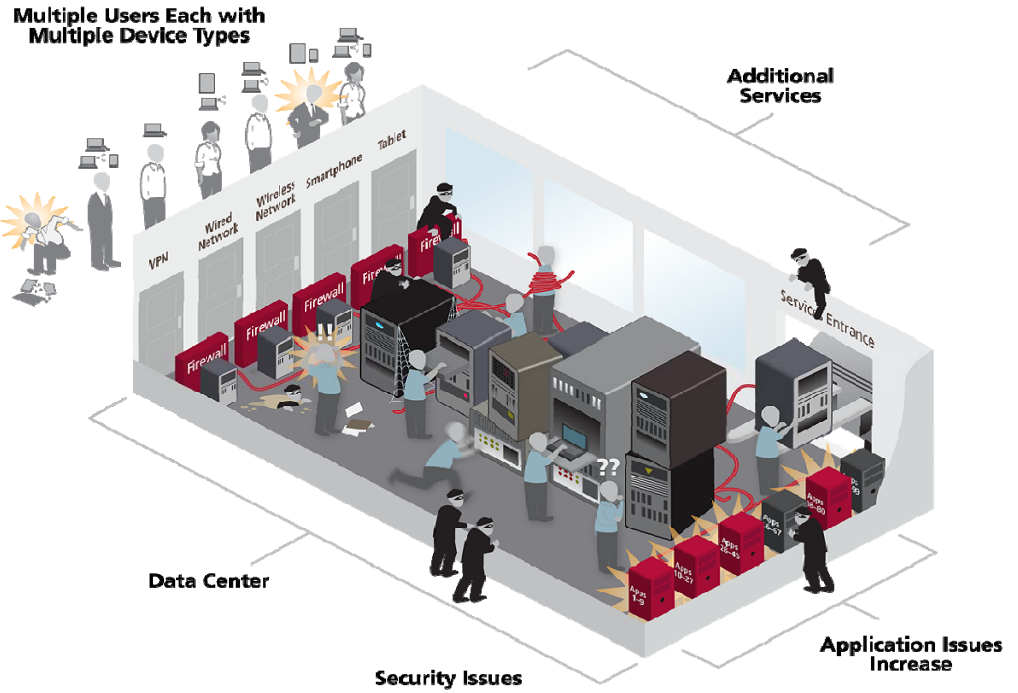
- It started simple
- More user types, services
- Application issues
- Security woes …



Static Datacenter

Complexity is the Enemy of Good Security

- What's the answer?

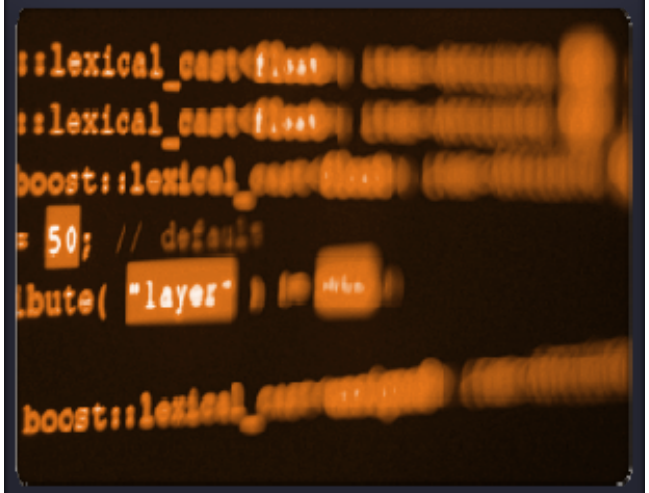


Attacks are Moving “Up the Stack”

Network Threats

90% of security investment focused here

Application Threats

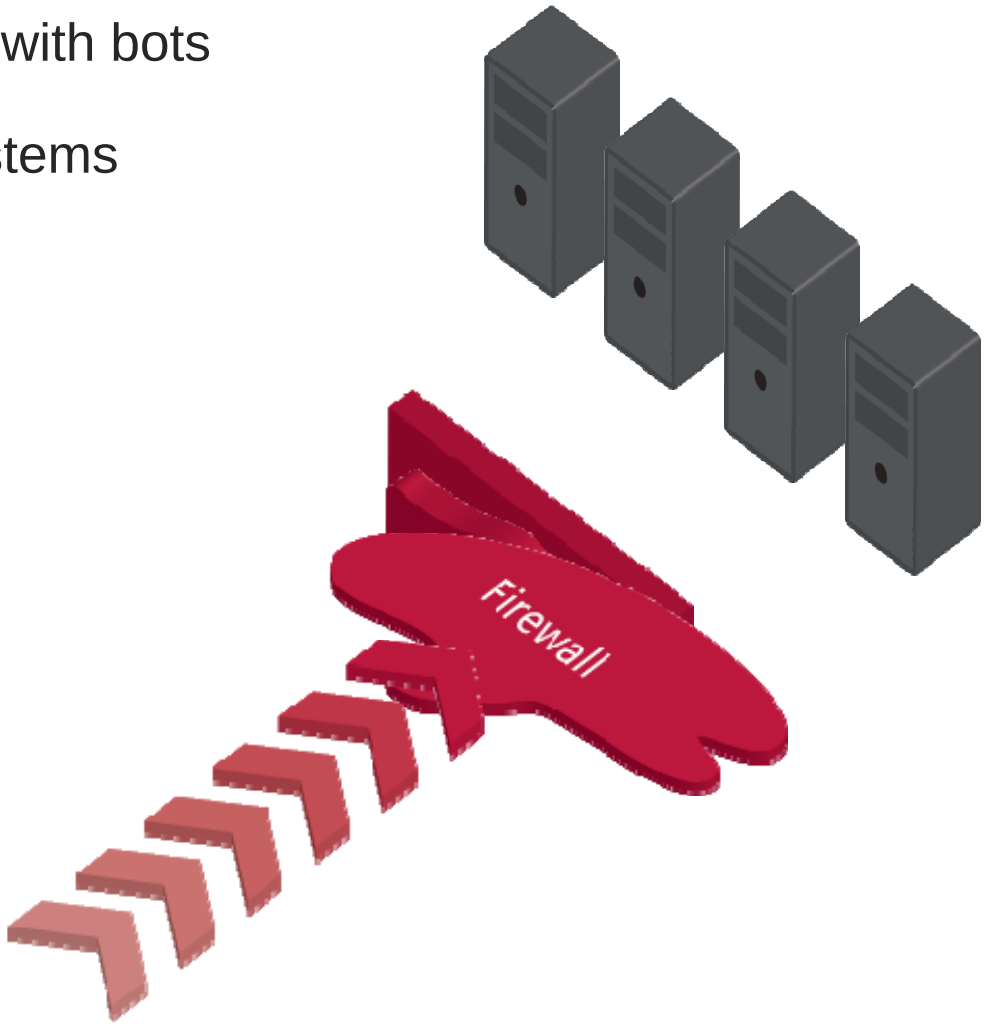


75% of attacks focused here

Source: Gartner

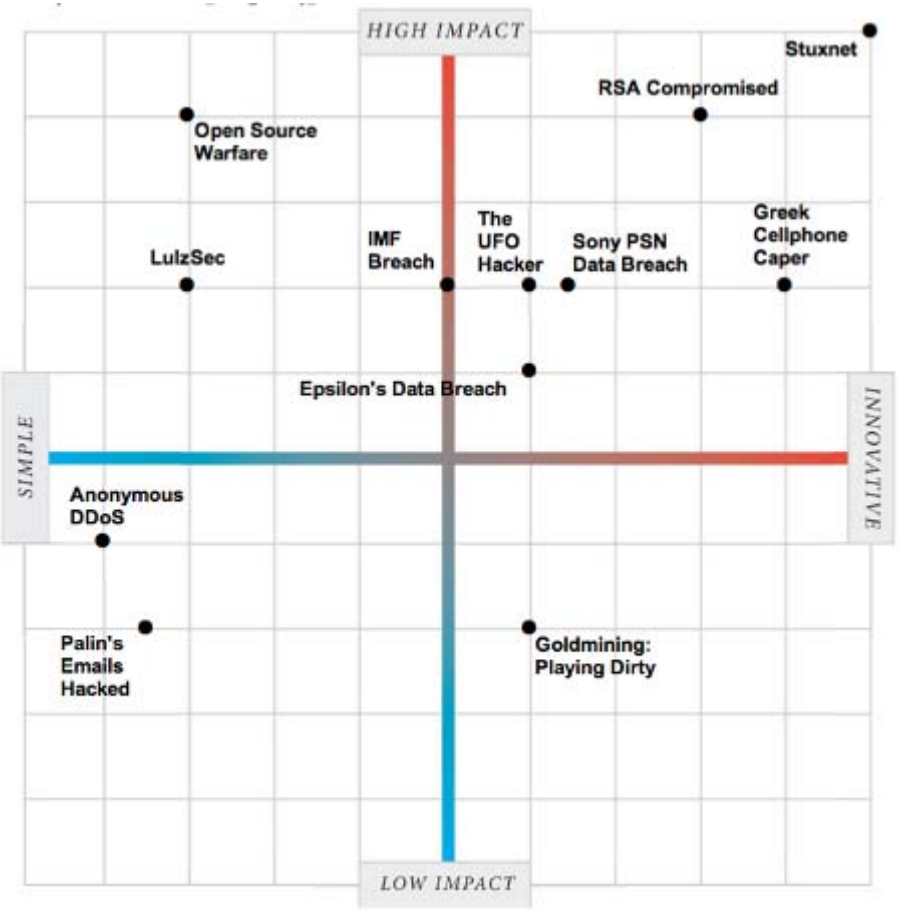
“Anonymous” Attack

- Anonymous targeted customer with bots
- Traffic attack melted legacy systems



Recent Application and Network Attacks

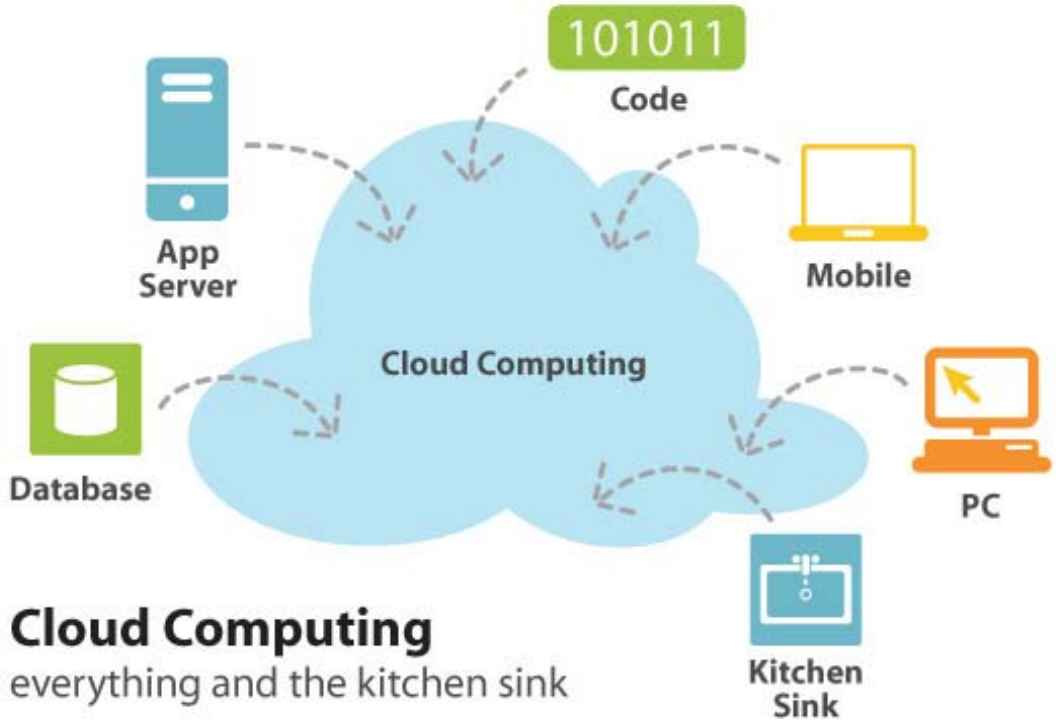
And the hits keep coming:



Source: http://spectrum.ieee.org/static/hacker-matrix

Challenges of Securing Dynamic Environments

Stats, Stories & Suggestions



spectrumfurniture.blogspot.com

What's the Risk? Where's the Threat?

What steps is Kiplinger taking to protect against future breaches?

We continue to monitor the situation closely and will adopt procedures and practices to minimize the risk of further incidents.

Threats are evolving, behaviors are changing

Figure 15. Threat action categories by percent of breaches and percent of records

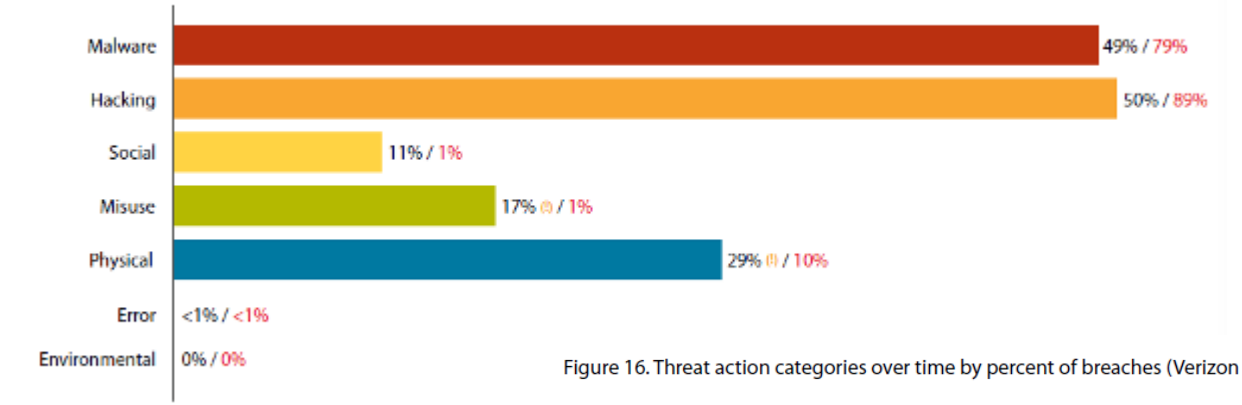


Figure 16. Threat action categories over time by percent of breaches (Verizon cases)

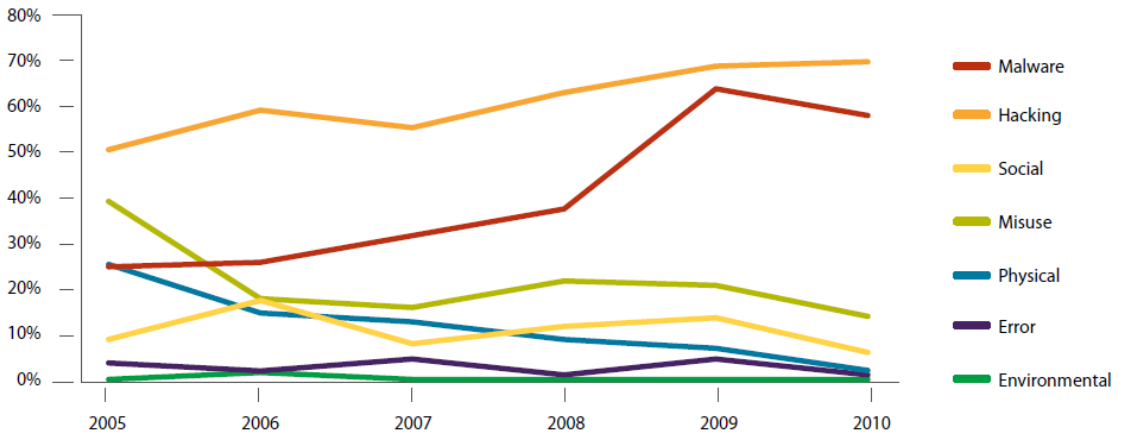


Figure 15 and 16: Verizon 2011 Data Breach Investigations Report

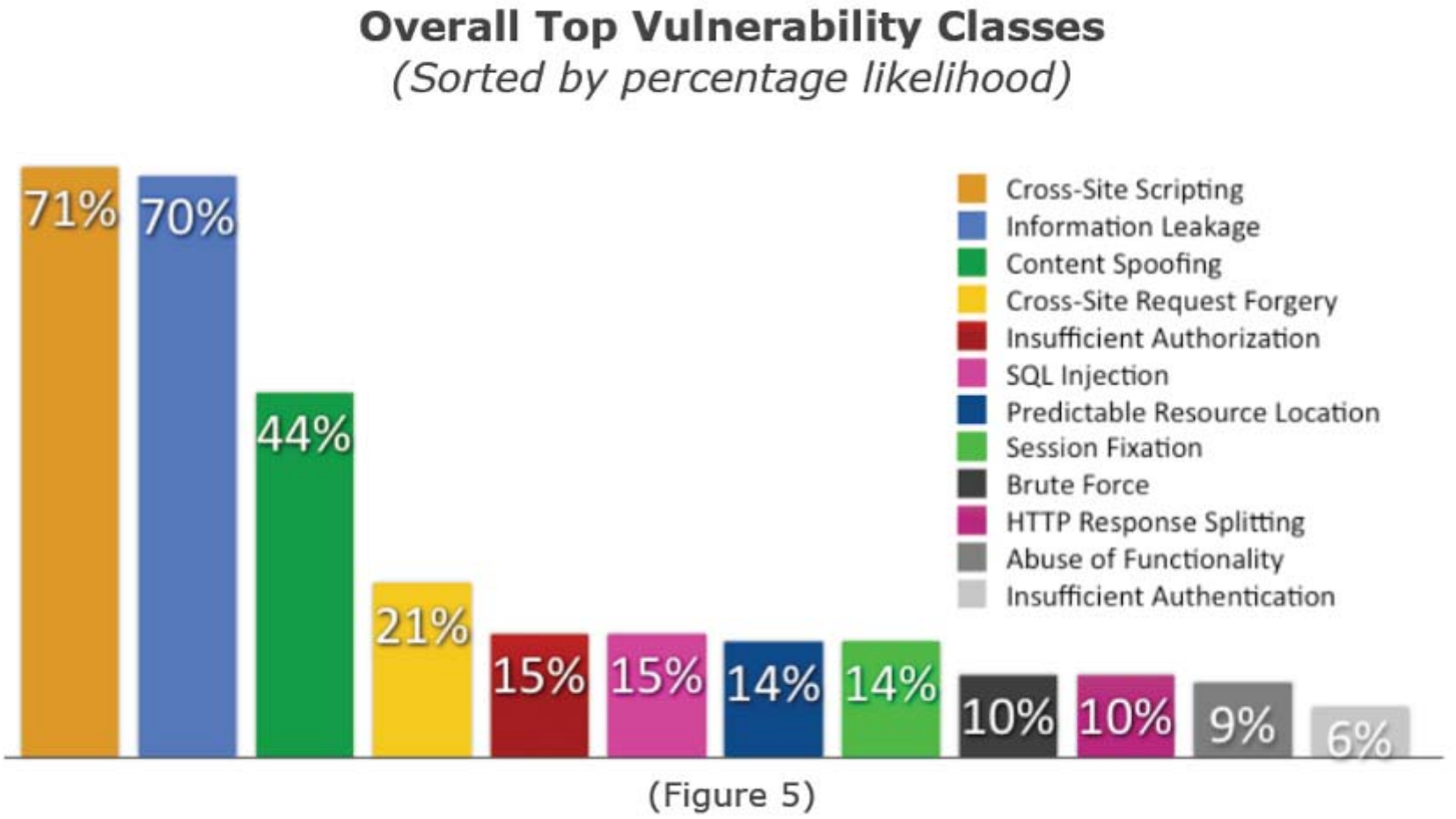
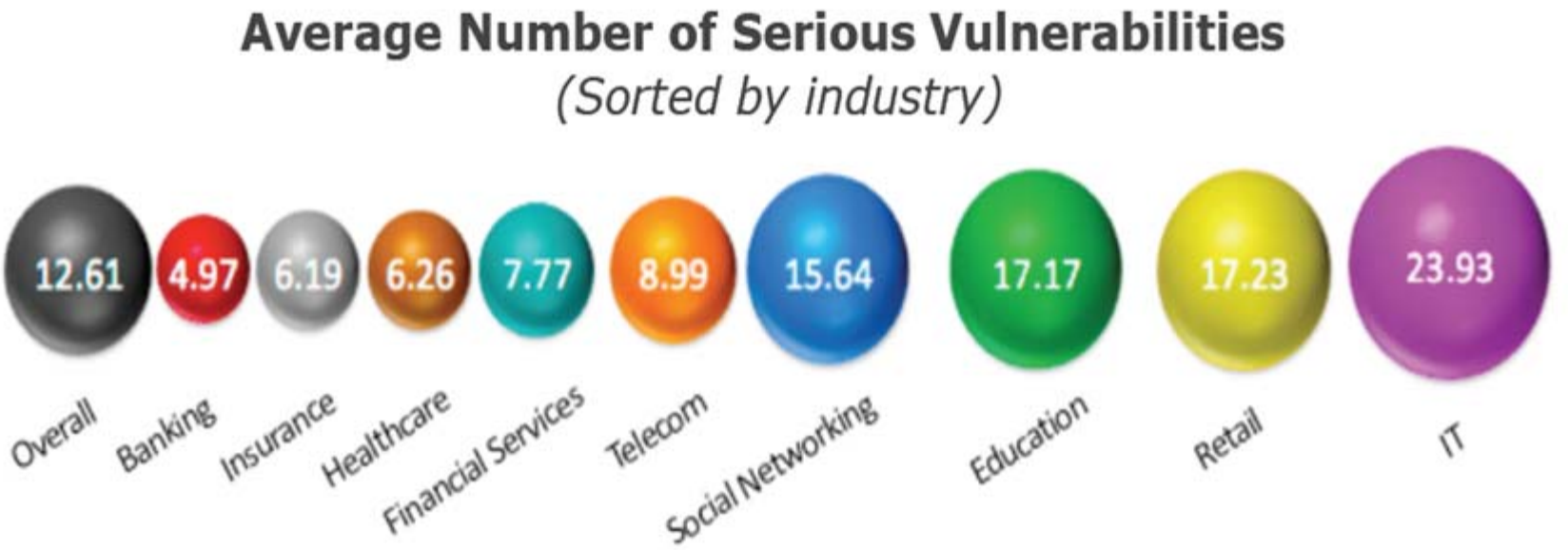


Figure 2 and 5: 10th Website Security Statistics Report (Q3 2010)



(Figure 2)

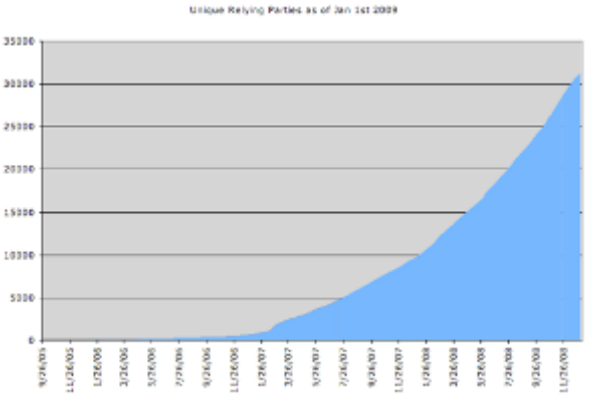
Figure 2 and 5: 10th Website Security Statistics Report (Q3 2010)

Always about being Secure

- **Security** a Big Concern for Cloud Computing
- **Security** Is Stunting Adoption of Cloud Computing
- Survey Finds Cloud **Security** Lacking
- **Security** experts ponder the cost of cloud computing
- 58% said ‘cloud technology does not provide adequate **security** safeguards’
- 60% of the financial services sector felt that cloud computing was not a priority or they were risk-averse to cloud computing.
- Identity, data management crucial to cloud success
- **Security** was the top concern with 73% saying such.
- 42% said that **security** concerns have prevented their adoption of cloud computing
- Preventing unauthorized access to company data was the biggest hurdle.

Authentication

- Digital Identity
- 81%:multi-factor authentication vital to securing the cloud
- Access Management based on Identity



PhoneFactor

Guests & Insiders

77% felt that their strategic partners had been weakened

50%+ organization isn't aware of all the cloud services

Insiders involved 70% to 80% of all IT crime

Evaluate all cloud activity - Cloud Inventory

Create a catalogue for employees

Examine providers for implications of blending of data

Create a policy around cloud computing

Ponemon Institute
Verizon
INC.com

CSO

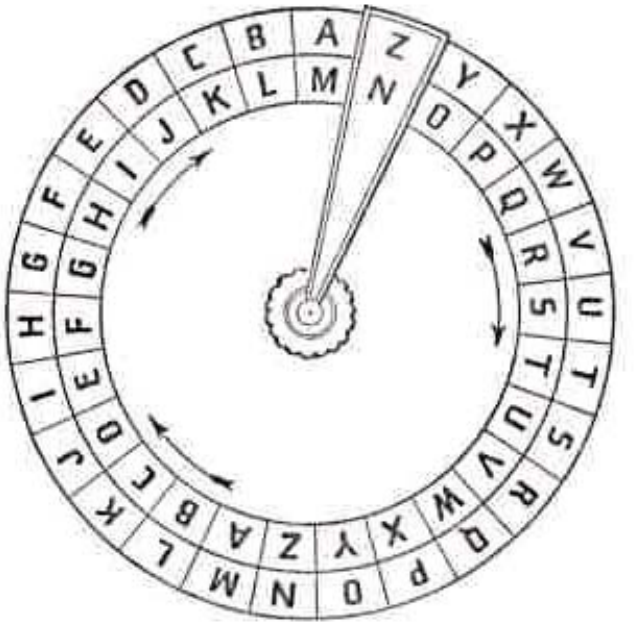
Encryption

84%:Encryption vital to securing the cloud

100% of TJX, Hannaford, Heartland

Recent breaches preventable

Policy



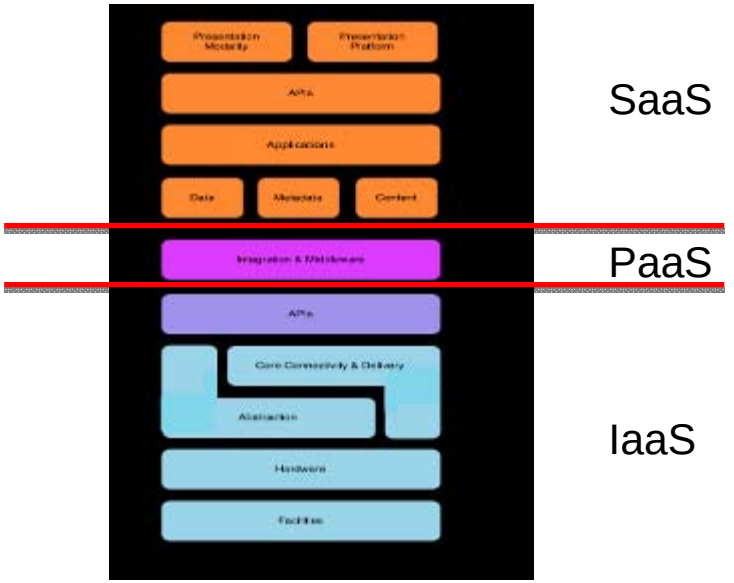
CODE WHEEL FOR REVERSE CODES

FireWall(s)

Different trust boundaries for IaaS, PaaS, SaaS

- **IaaS**: entire infrastructure from facilities to HW
- **PaaS**: application, Middleware, database, messaging supported by IaaS
- **SaaS**: self contained operating environment: content, presentation, apps, mgt

80% Intrusion prevention is vital to securing the cloud



Keys – aka PKI

Enabling technology for an identity ecosystem

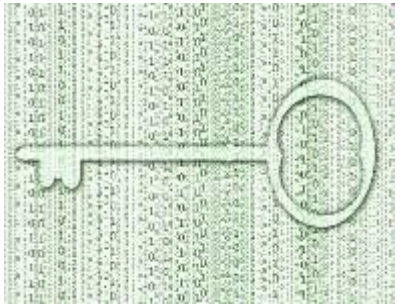
87% concerned about personal identifying & financial info

Management challenges involved in securing PII

Encrypt data in transit, at rest, backup media

Secure key store

- Protect encryption keys
- Limit access to key stores
- Key backup & recoverability (test)



Management (Cloud & Risk)

71% want a tool that managed all their infrastructure

Avoidance: eliminate conditions that allow the risk to be present

Acceptance: acknowledge the existence but don't do anything except for a contingency plan

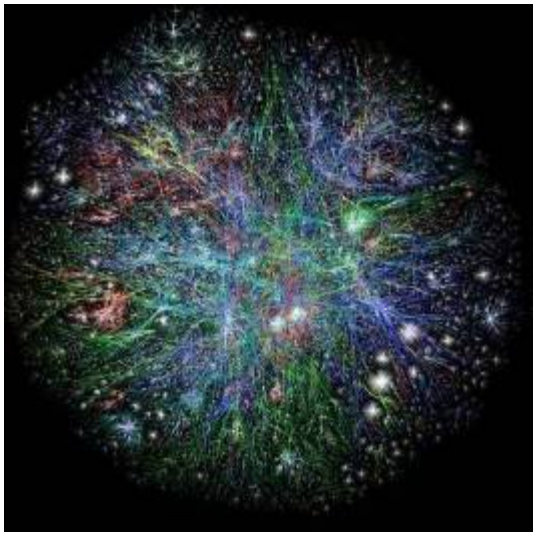
Mitigation: minimize the probability or impact of the risk

Deflection: transfer the risk somewhere else

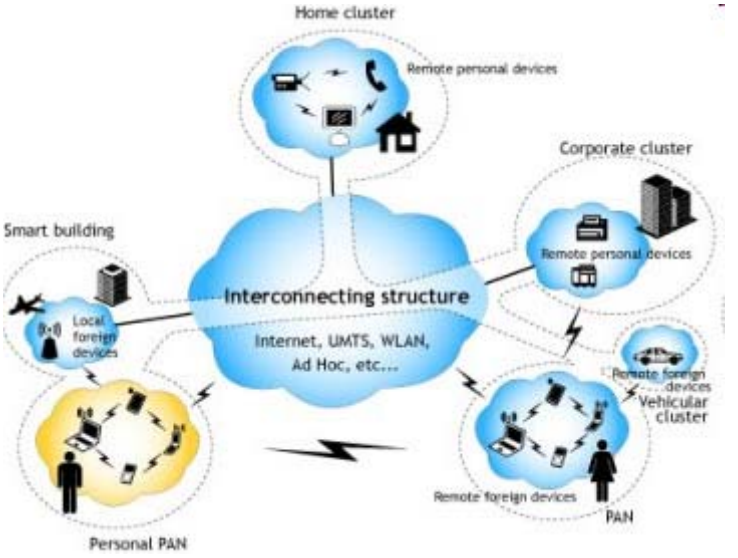
Zenoss

Networks

- Burst up/down bandwidth on demand
- Connect servers for auto movement of VMs
- Provide visibility in a dynamic environment



Drive Identity into the Network



TCP/IP v6

- Chips
- Seamless user experience
- Scale and Connectiveness
- IPv4, IPSec is optional
- IPv6, IPSec support is mandatory
- Confidentiality: Traffic is encrypted
- Authentication: Digitally signed
- Data integrity: Packet not modified

Reliability

Availability is a key metric

Cloud performance issues costing firms €600,000 a year

Companies struggling with cloud performance

Cloud apps cost firms £500,000 a year in poor performance

Compliance

Full responsibility

- who can access data
- who sees it
- how it is stored
- federated reporting

Integrity and security

The Platform - vulnerabilities that can be exploited?

What happens if you stop using a cloud service?

How do you know data is really deleted?

Who has access to the application and data?

What access rights do privileged users have?

Private Cloud

- 58% either using private clouds or planning to do so
  - 15% devote >20% of their IT budgets to cloud computing
- 89% believe private clouds are the next step to implementing virtualization
- 43 % planning a combined approach of private & public cloud
- 76% showed more confidence in internal IT departments for providing data security than outside vendors
- 91% vs 50% concerned about security issues
- 86% believe data is more secure in a private cloud

- Virtualization
- Data center automation
- Chargeback metering
- Identity-based

InformationWeek, Novell

You, the user

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is right now, it's going to get much scarier," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

Zzzzzzzzzzzzzzzz

Data Security (24%)

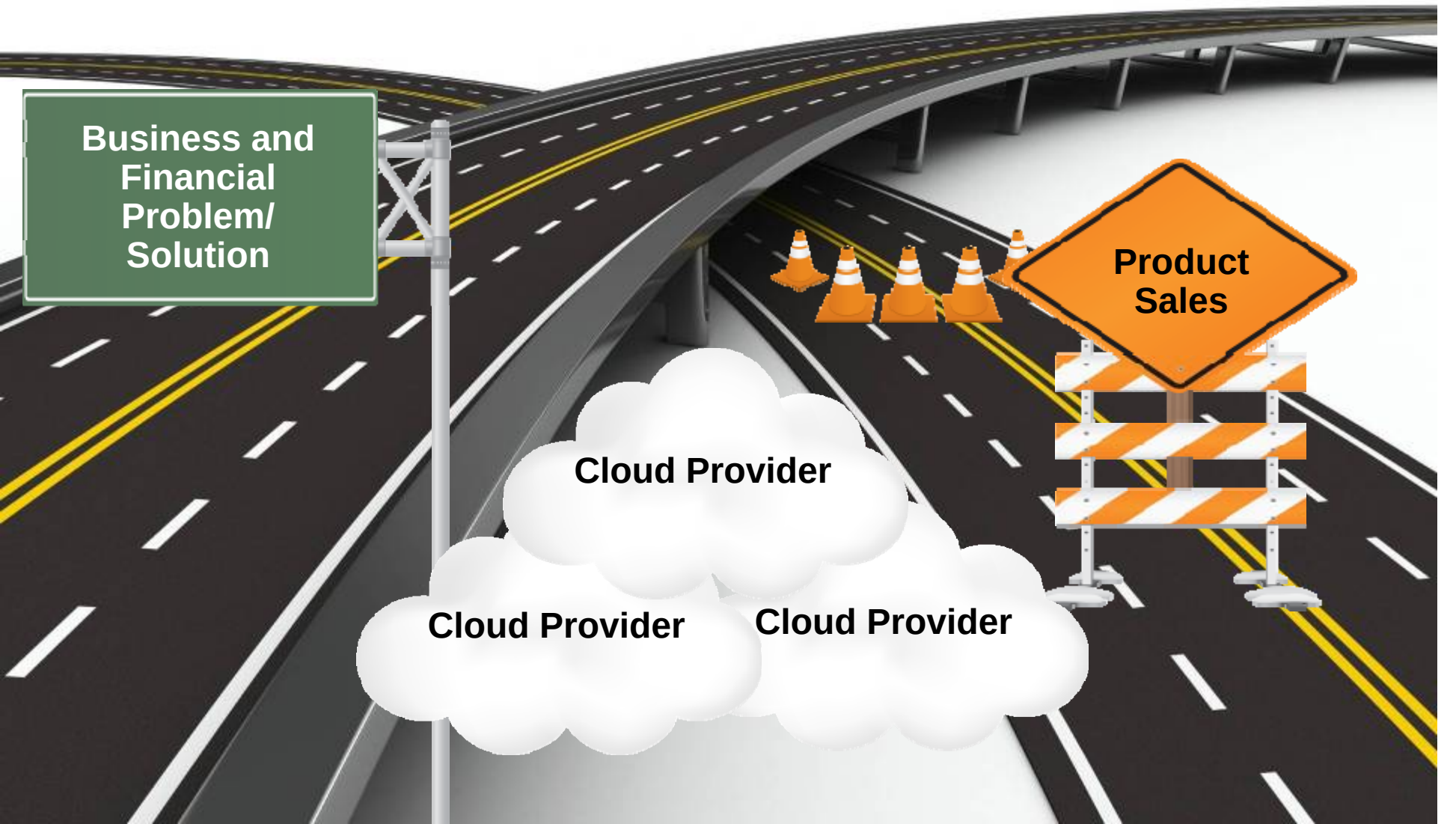
Hardware and/or OS upgrades (13%)

Heavy workloads (10%)

Sufficient budgets to fund IT projects (10%)

Keeping pace with technology innovation (9%)

Network World - 1,400 U.S. CIOs


Business and Financial Problem/ Solution
Product Sales
Cloud Provider
Cloud Provider
Cloud Provider

How to Improve security?

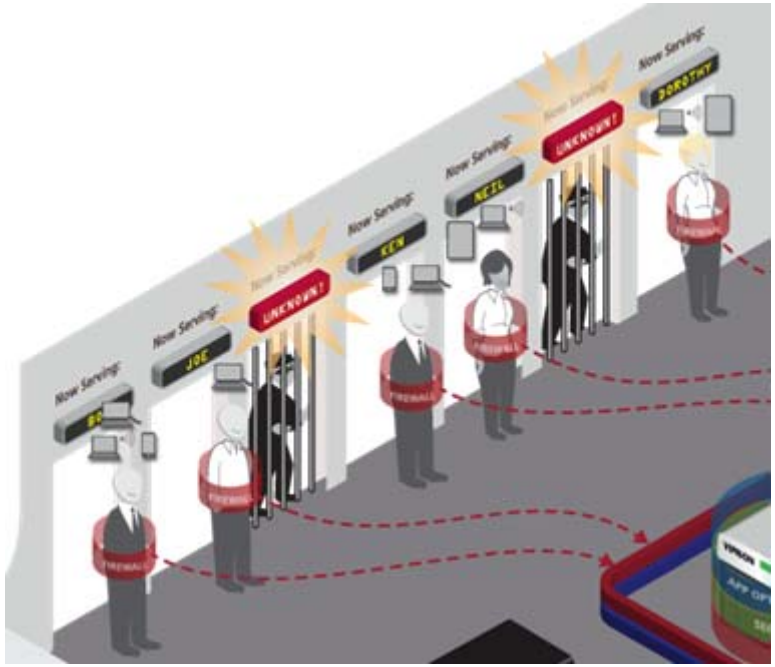
When?
Office Hour

Where?
Hong Kong

Who?
2-factors auth

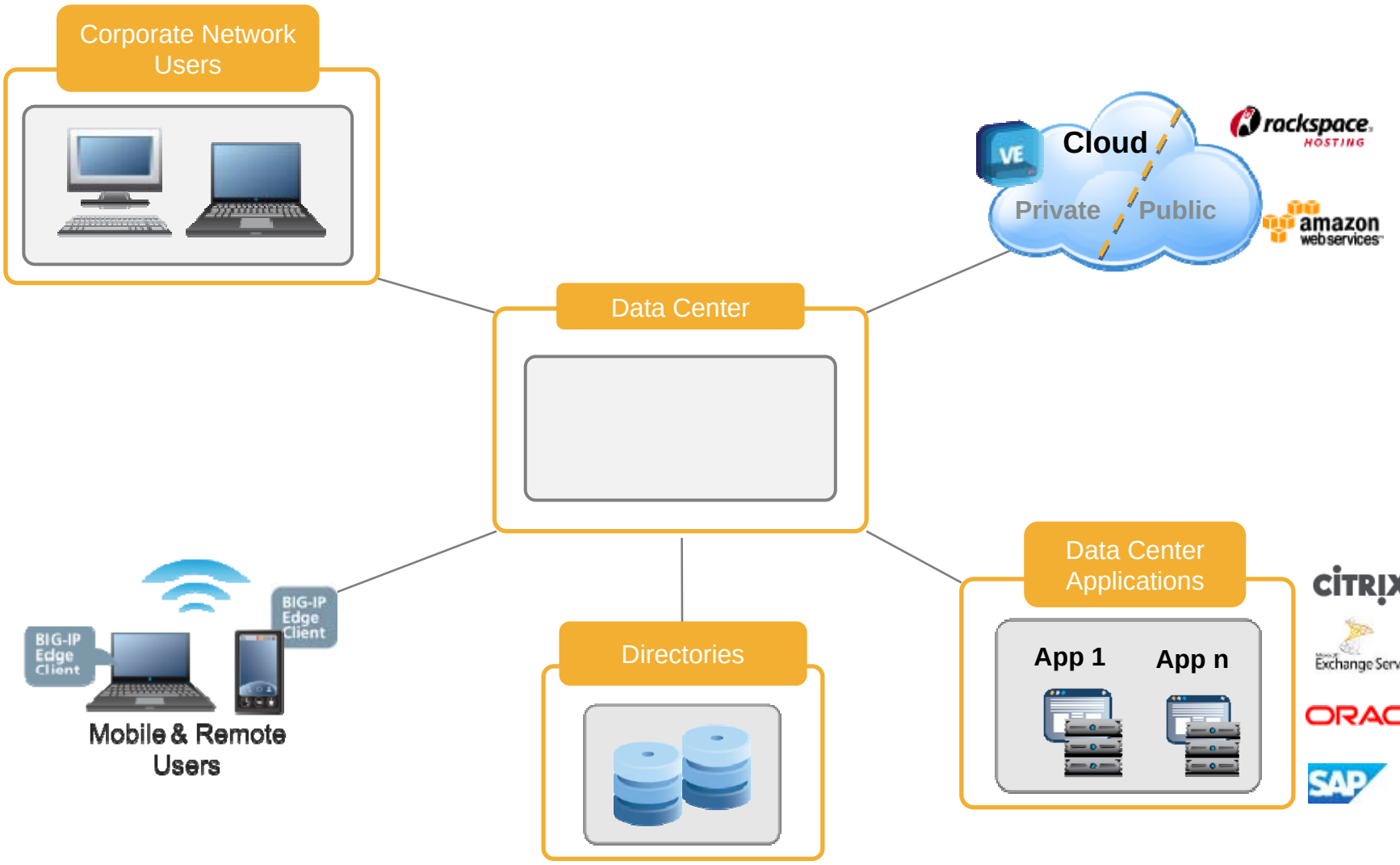
How?
Only trusted devices

5 W Rules



- **When** do the Services Available ?
- **Who** is accessing ?
- **What** devices are requesting access ?
- **What** applications were accessed ?
- **Where** did the user navigate ?

Enterprise and Service Provider IT



End

Thank You !