

Single Points of Failure in the Cloud

Presented by:

Ram Mohan

Chief Technology Officer

rmohan@afilias.info



 @Afilias

Who is Afilias?

- **10 years of experience** in critical Internet infrastructure and DNS
- Best known for domain name registry services in **support of 17 million domains** across 15 TLDs
- Diverse DNS Network handling **billions of queries** daily



Platforms, Markets & Innovation

Cloud Computing is a clear representation of the shift to Products as Services

The ability to monitor, measure and customize and bill for asset use at a fine grained level means services can be created around products.

**Cloud Computing is a platform and mind shift,
not a just a technology shift**



Cloud Computing

BENEFITS & CHALLENGES

Why use Clouds?

FOR:

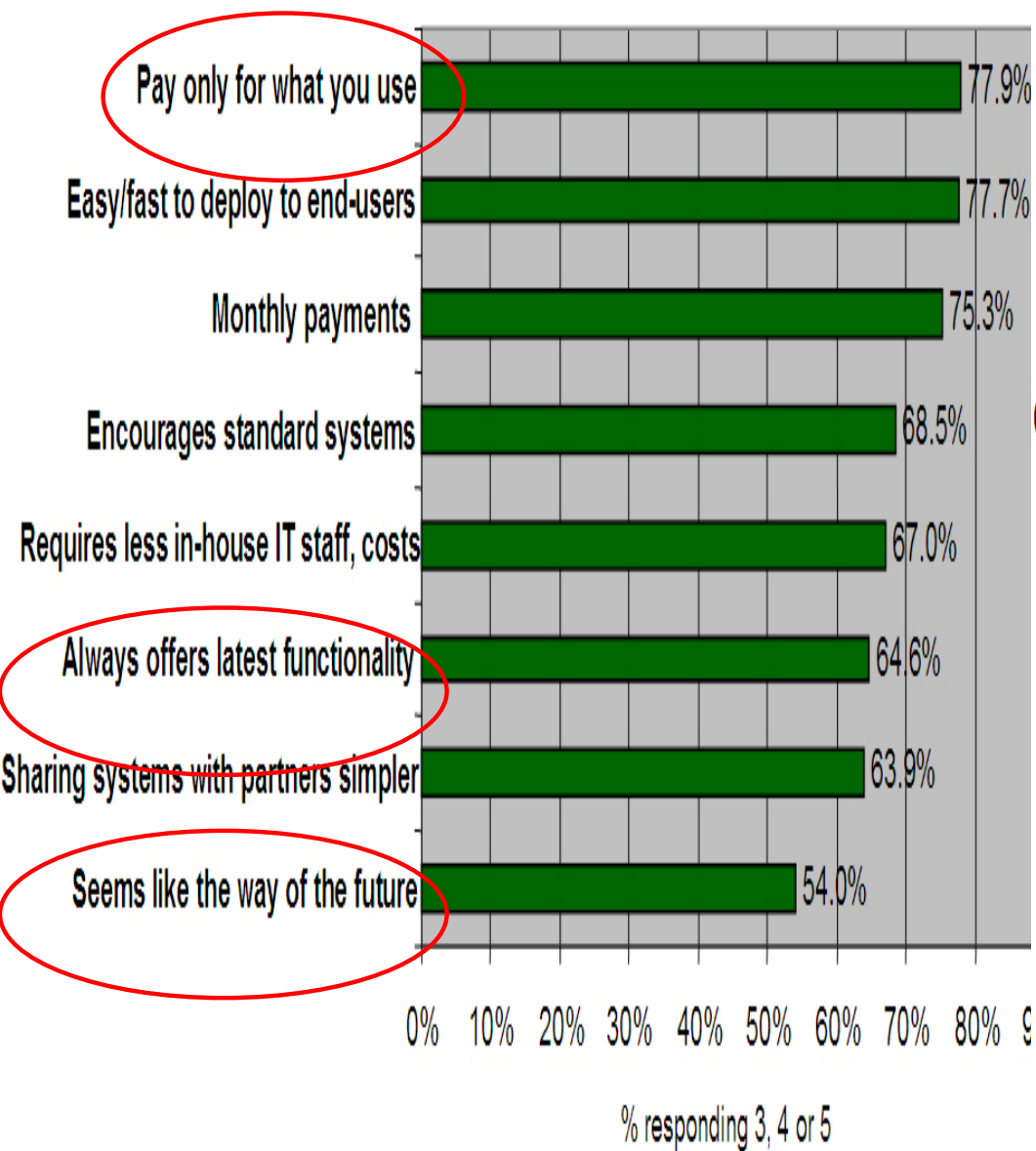
- Service managed by experts
- Process efficiencies
- Scalability
- No maintenance or coding
- No infrastructure
- “Pay for what you use”

AGAINST:

- Loss of control
- Dependence on DNS
 - Data leakage risk
 - Risk of downtime
- Open to Security exploits

Q: Rate the **benefits** commonly ascribed to the 'cloud'/on-demand mo

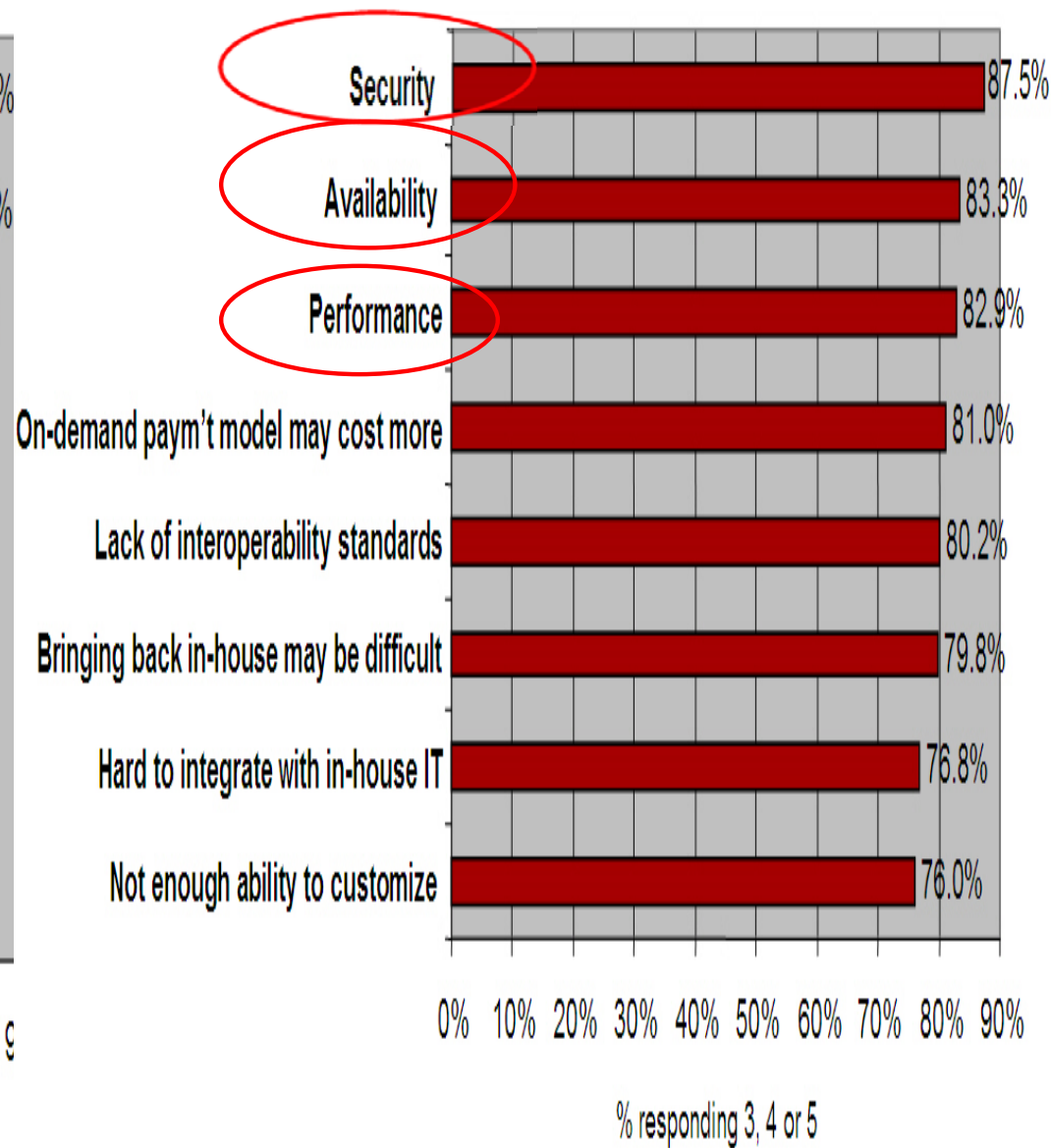
(Scale: 1 = Not at all important 5 = Very Important)



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

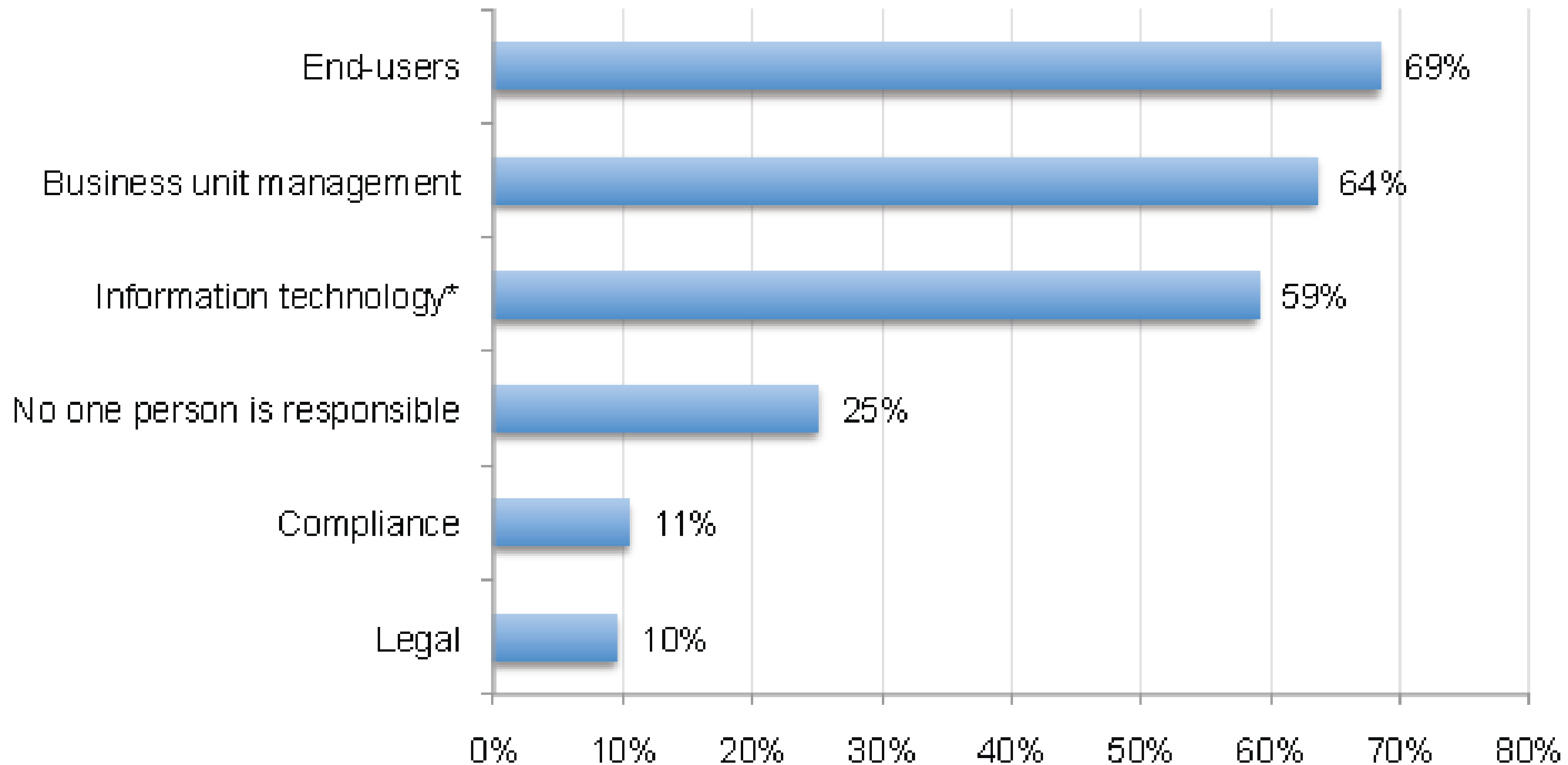
Q: Rate the **challenges/issues** of the 'cloud'/on-demand model

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



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

Who is most responsible for cloud security?



Source: [Ponemon Institute & CA](#), May 2010



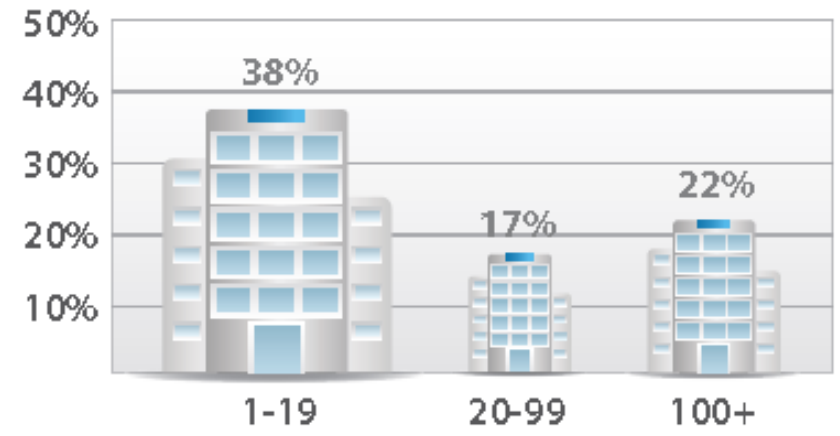
Cloud Computing

ADOPTION OF THE CLOUD

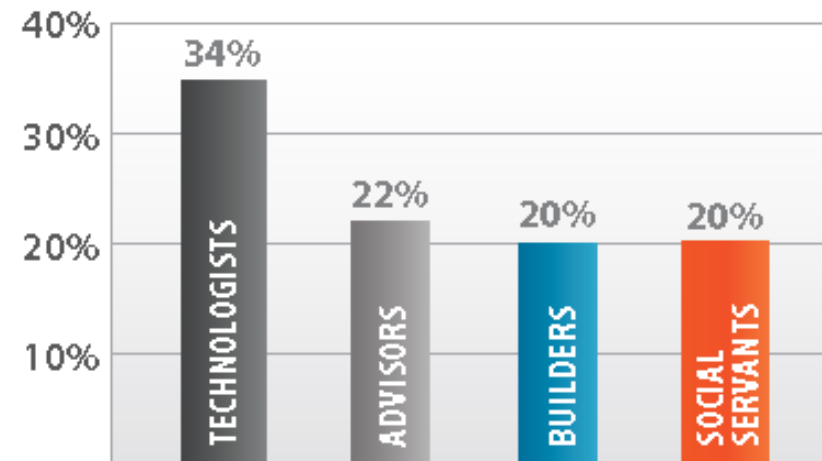
Who Is Using The Cloud?



Cloud Deployment by Region



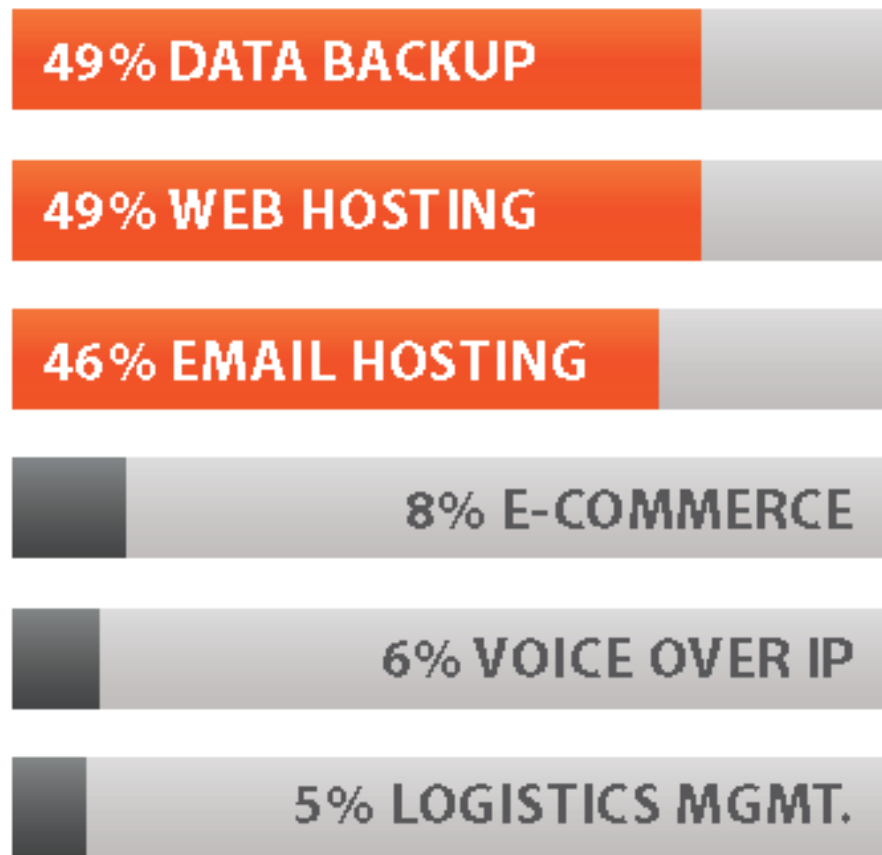
Cloud Deployment by Company Size



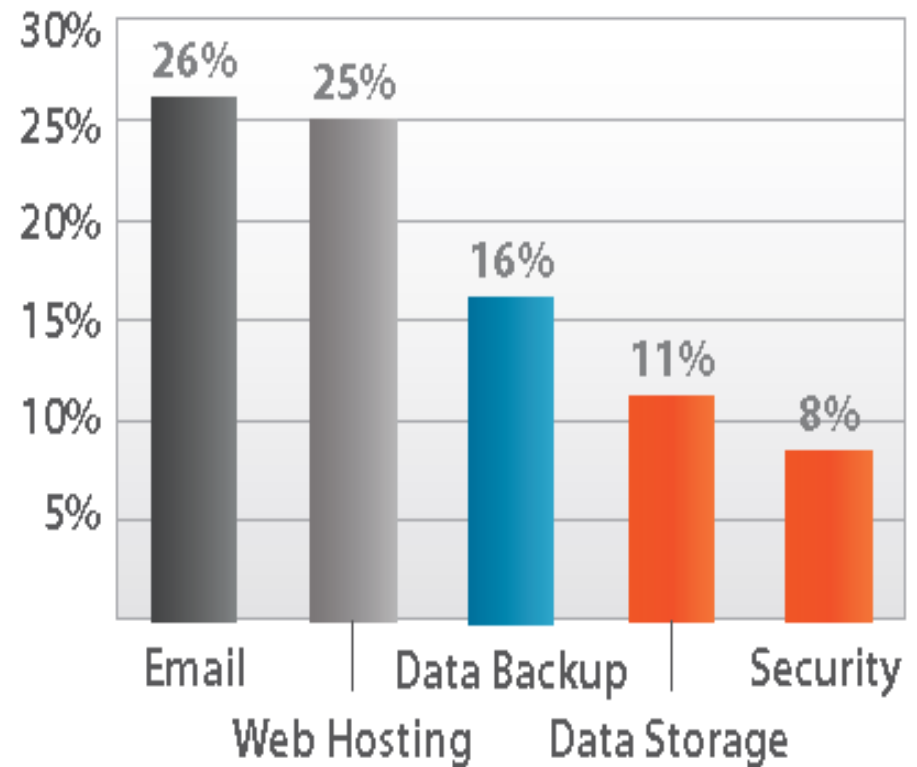
Cloud Adoption by Industry Group

Source: SpiceWorks, July 2010

What is the Cloud Being Used For?



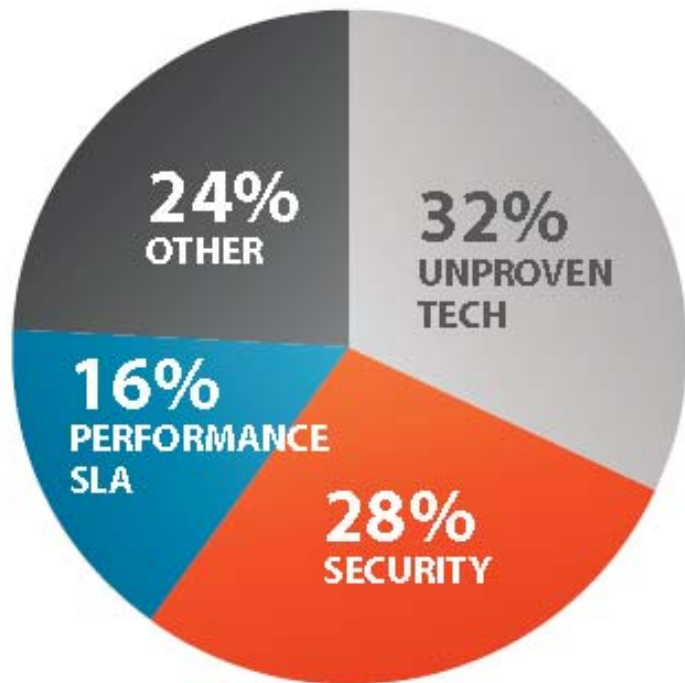
Adoption by Type of Service



Cloud Deployment by Service

Source: SpiceWorks, July 2010

What are the concerns regarding Cloud Deployment?



Cloud Deployment Concerns

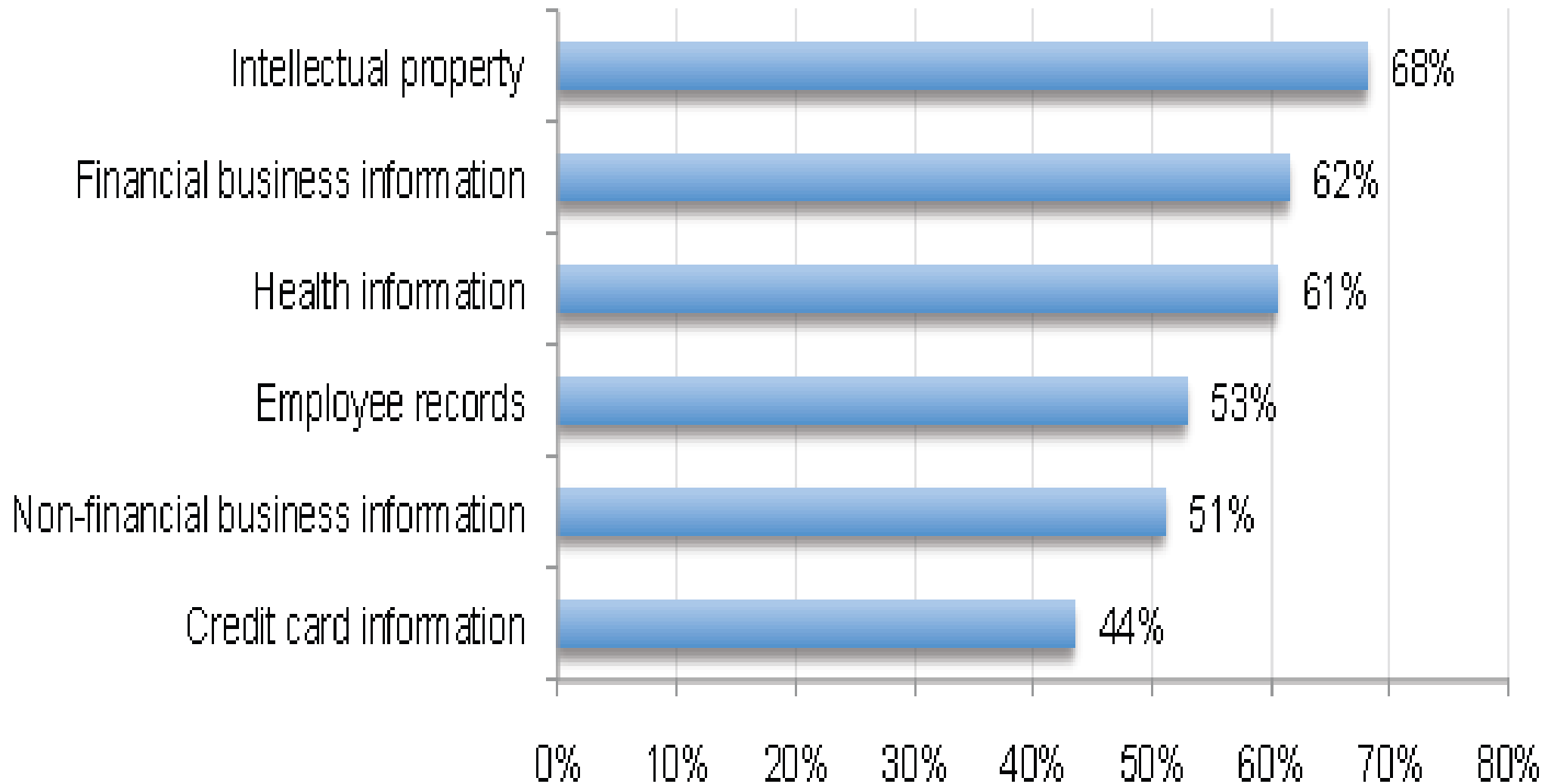
Adopters vs Non-Adopters



Cloud Concerns by Adoption Group

Source: SpiceWorks, July 2010

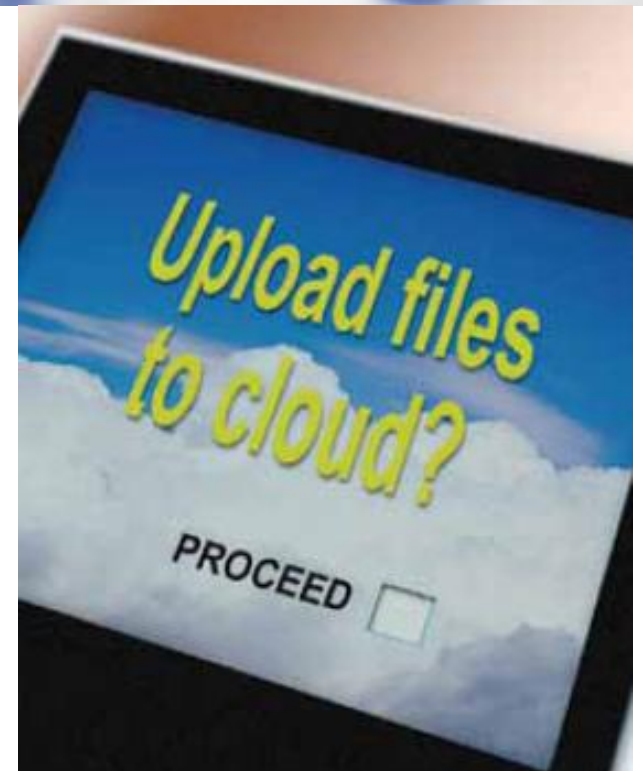
What is too risky for the cloud?



Source: [Ponemon Institute & CA](#), May 2010

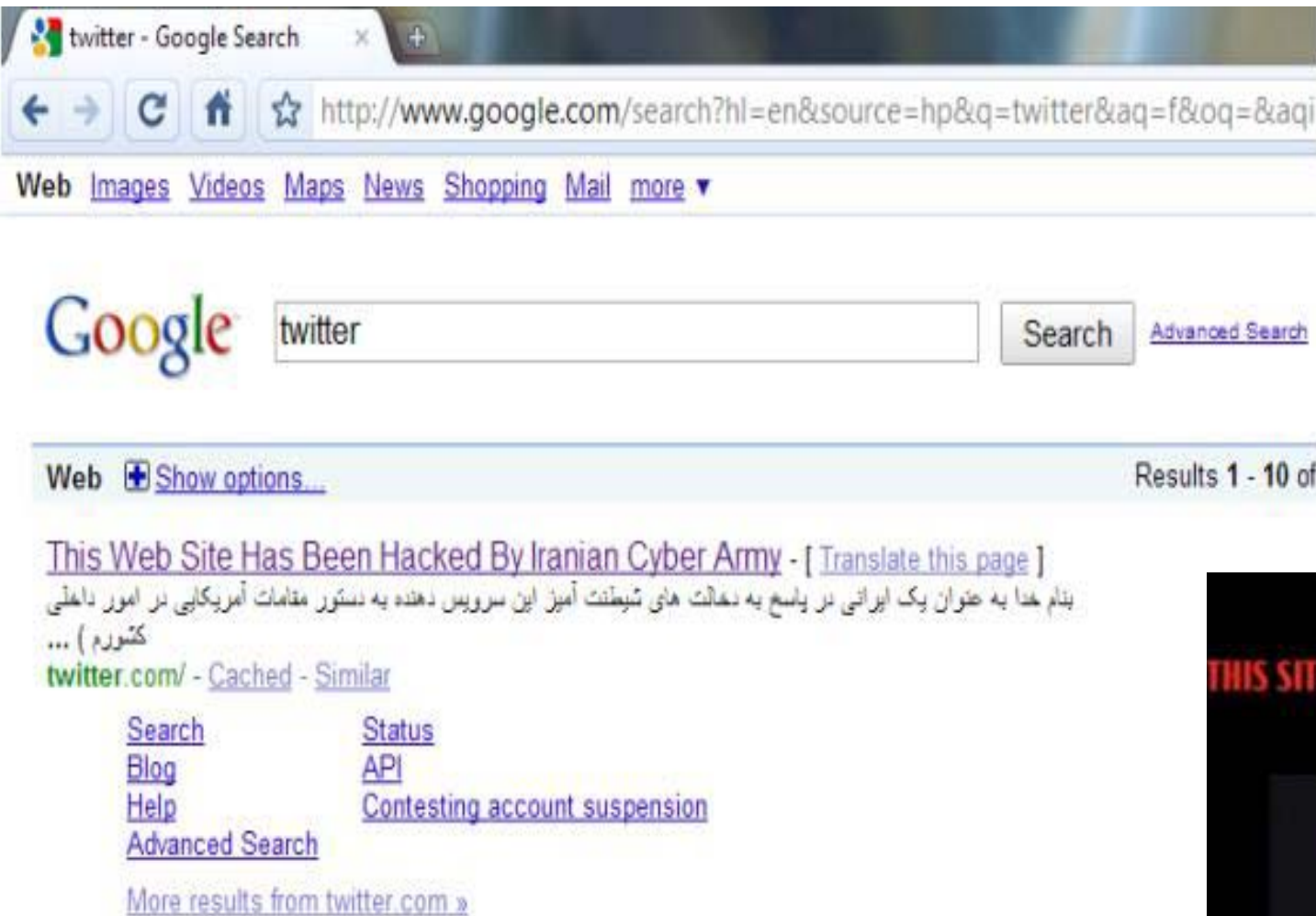
Cloud Computing

ATTACKS



CASE EXAMPLE:

Twitter – Attacked Through The Cloud



twitter - Google Search

http://www.google.com/search?hl=en&source=hp&q=twitter&aq=f&oq=&aqi

Web Images Videos Maps News Shopping Mail more ▾

Google twitter Search Advanced Search

Web Show options... Results 1 - 10 of

[This Web Site Has Been Hacked By Iranian Cyber Army](#) - [[Translate this page](#)]

بنام خدا به عنوان یک ایرانی در پاسخ به دخالت های شیطنت آمیز این سرویس دهنده به دستور مقامات آمریکایی در امور داخلی کشورم (...

[twitter.com/](#) - [Cached](#) - [Similar](#)

Search	Status
Blog	API
Help	Contesting account suspension
Advanced Search	

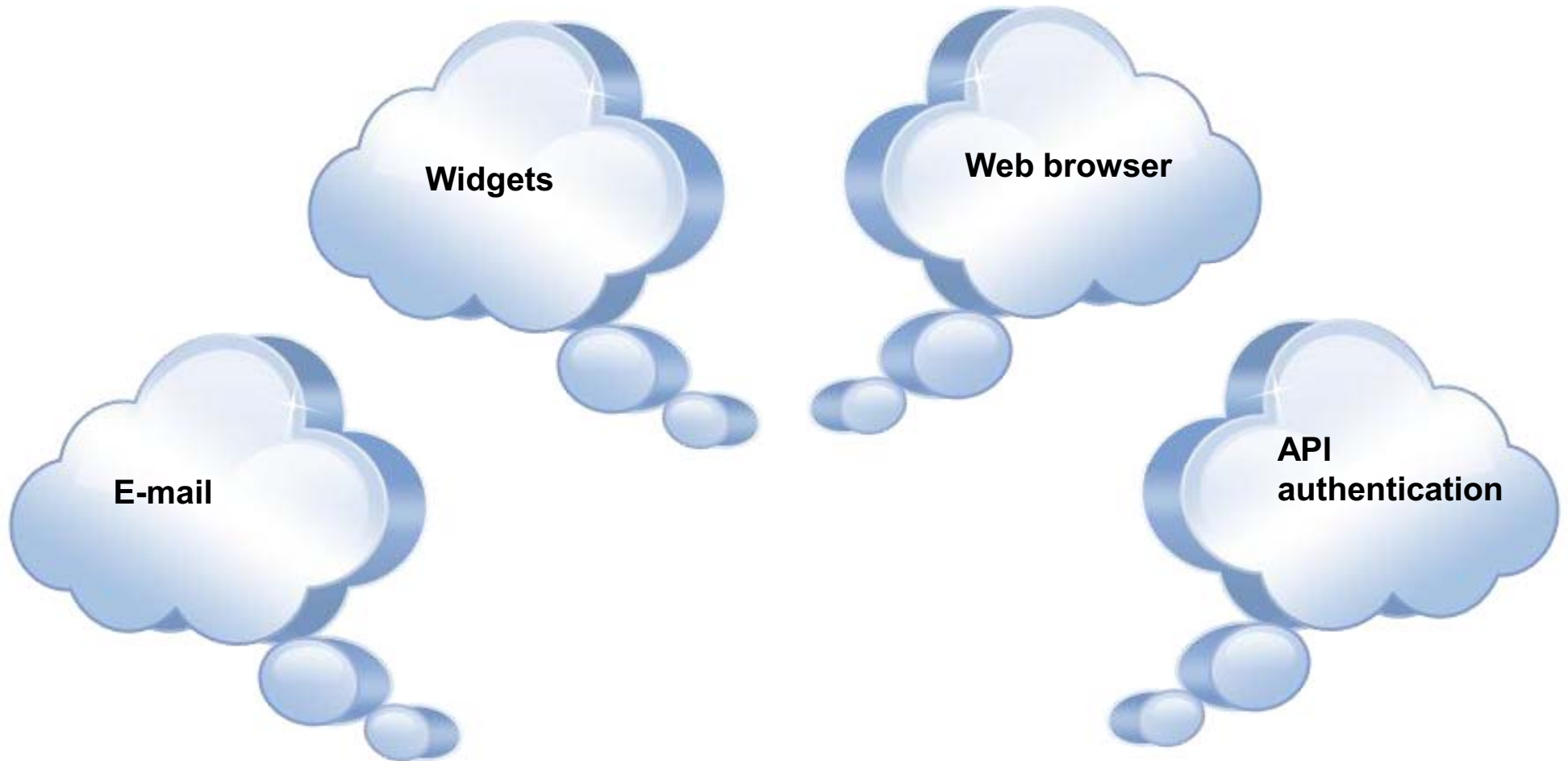
[More results from twitter.com »](#)

twitter



Source: Ram Mohan, [CircleID](#)

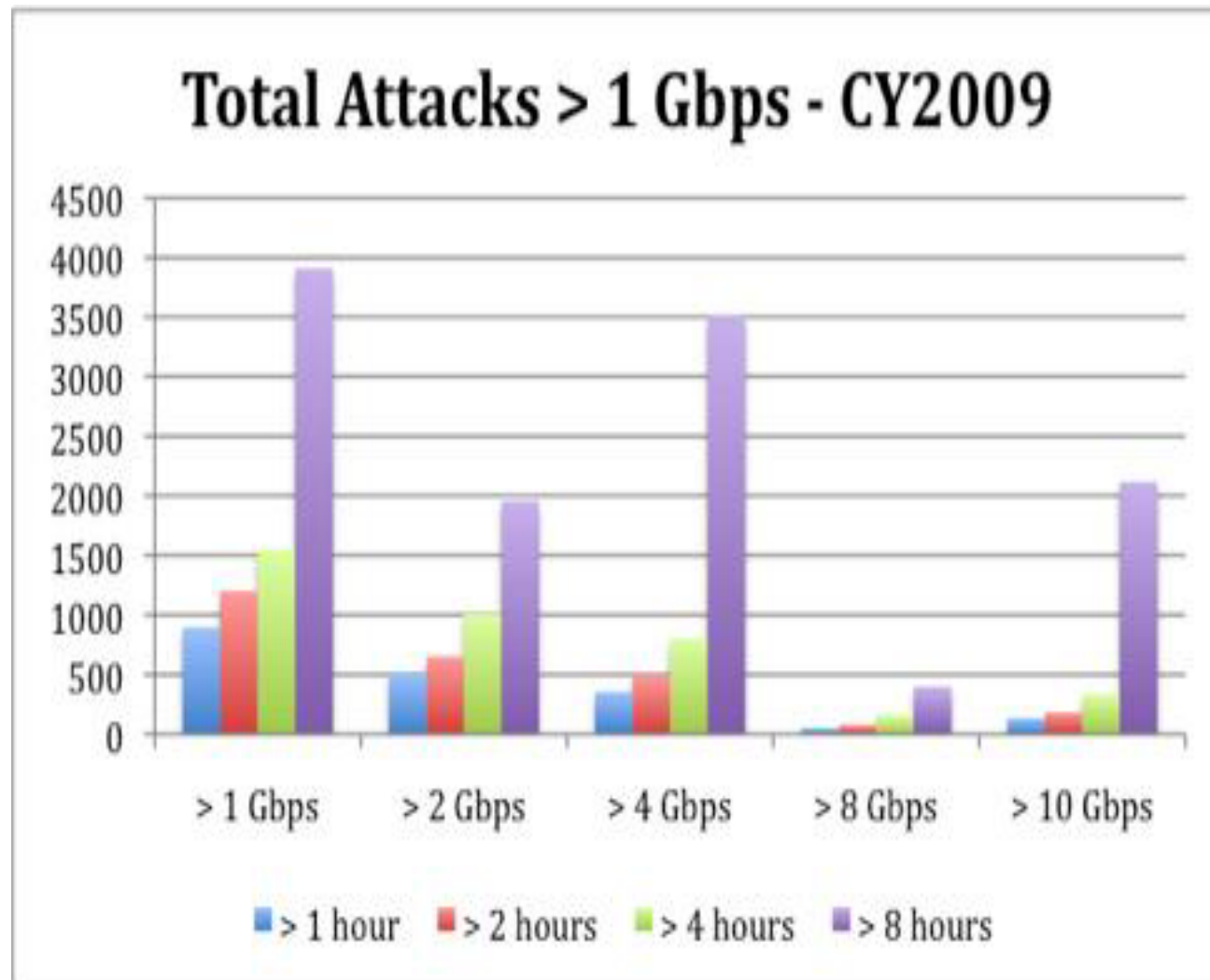
Cloud depends on DNS



DNS is a single point of failure

Most attacks are “long and heavy”

- Attacks are shifting to the Cloud
- Growth in >1 gbps attacks targeting applications, specifically DNS, load-balancers or SQL-backed infrastructure.



Source: Arbor Networks <http://asert.arbornetworks.com/2010/01/fire-or-ddos-which-is-more-probable/>

DDoS Attacks Are Growing

Largest DDoS Attack – 49 Gigabits Per Second

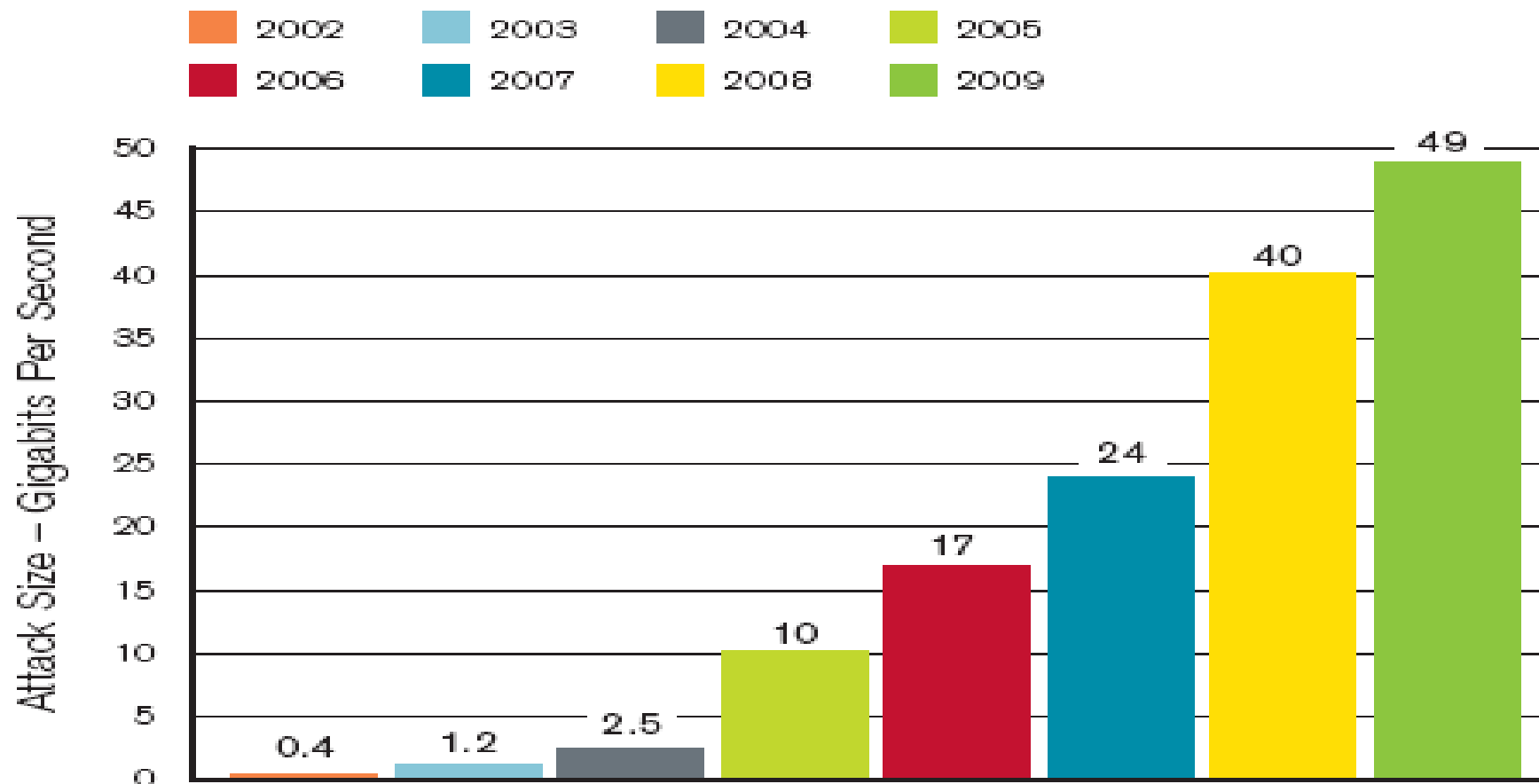


Figure 1: Largest DDoS Attack – 49 Gigabits Per Second

Source: Arbor Networks, Inc.



Cloud Computing

SINGLE POINTS OF FAILURE

DNS

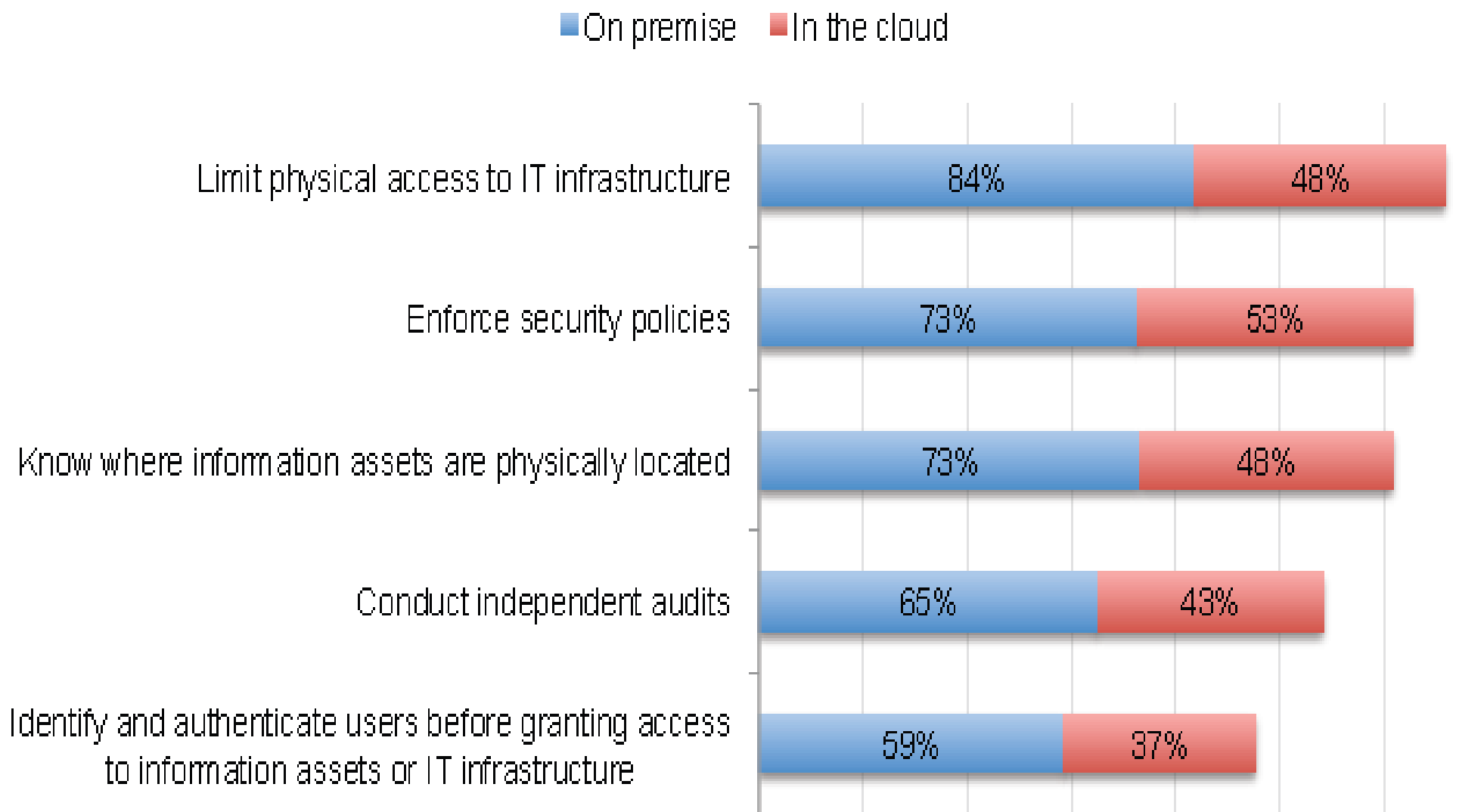
- Threats to the DNS are growing
 - Networks that permit access to Cloud-based services are increasingly coming under attack
 - DDoS is fastest growing and most significant issue
- The number of vulnerabilities is expected to double in 2010 compared to last year.



DNS networks need to be based on:

- 1. a stable, reliable security model to thwart criminal attacks**
- 2. a diverse, scalable network that avoids single points of failure**

Security Features With Most Difference In The Cloud vs. On Premise



Source: [Ponemon Institute & CA](#), May 2010

Identity and Access Management

- Securing Access Rights is probably the single easiest point of failure to fix
 - Is also likely the largest single point of failure
 - Authenticate using appropriate tokens
- Lack of uniform access rights procedures and lack of standardization is likely to result in more exploits over the next year

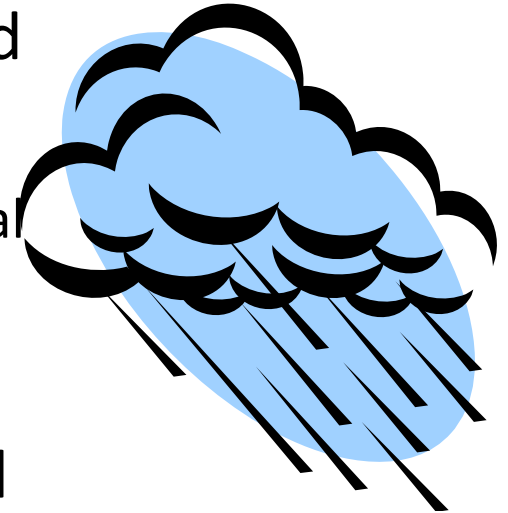


Identity and Access Management must:

- 1. Effectively manage access rights, especially for privileged users**
- 2. Restrict privileged user access to sensitive data**

Electronic Discovery, Compliance

- Compliance and electronic discovery in a cloud system could get tied up with a single vendor
 - Vendor cooperation may impact your organizational ability to comply with regulation or laws
- Logs and other routine but required information may not be available on the cloud unless specifically provisioned



Electronic Discovery and Compliance must:

- 1. Provide measures to investigate inappropriate or illegal activity**
- 2. Permit 3rd party access to parts of the cloud for compliance, forensics or audit**

Encryption and Key Management

- To achieve effective secure cloud computing
 - Granular encryption is needed – at file level
 - Group based policies
 - Centralized key and policy management



Centralized key and policy management might be useful

Encryption and Key Management regimes should:

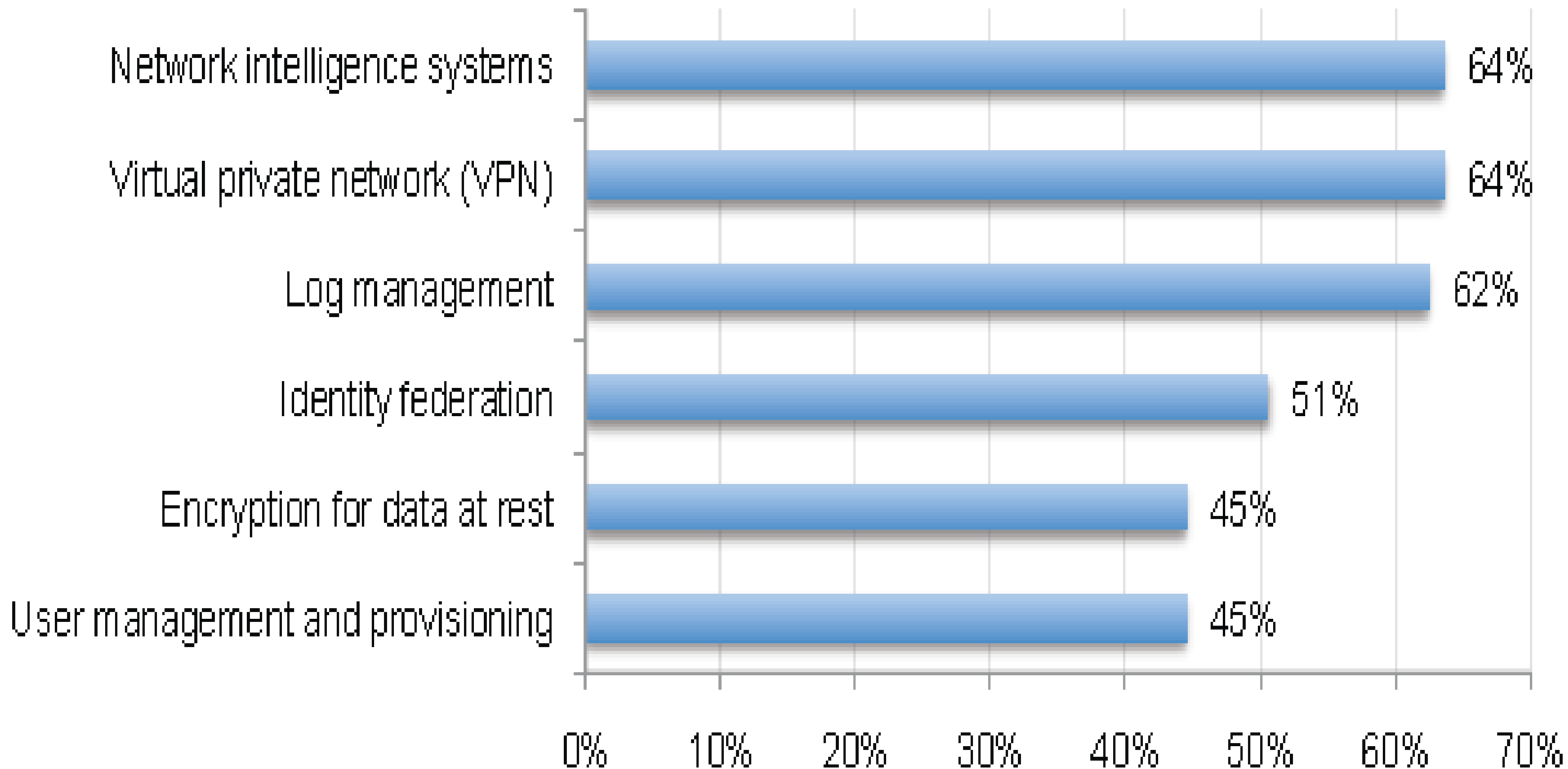
1. Go for granularity
2. While retaining group based policies



Cloud Computing

RECOMMENDATIONS

Some Important Cloud Secure Technologies



Source: [Ponemon Institute & CA](#), May 2010

Recommendations

1. Build an inventory of all cloud computing resources in use today
2. Begin risk assessment of cloud deployment solutions in use
 - If high risk, decide on course of action
3. Develop policies and procedures
 - Rate and rank cloud computing providers
 - Begin mitigation strategy for single points of failure
4. Move mission-critical applications to a secure cloud environment only after single points of failure are mitigated or eliminated



Thank you!

QUESTIONS?

Ram Mohan
Chief Technology Officer
rmohan@afilias.info