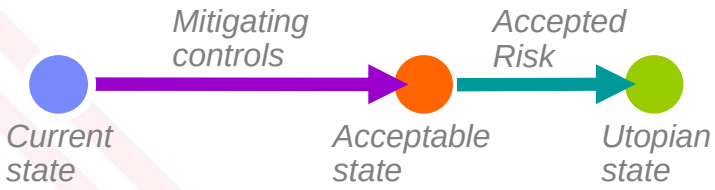
IBM IT Risk Management Seminar

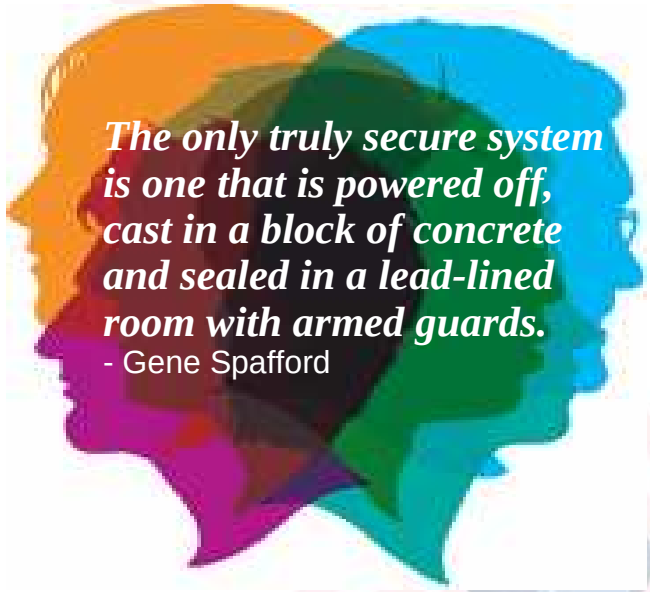
New Risks in the New World of Emerging Technologies

Victor Chu
Client Technical Professional
Identity, Security, and Compliance Management
Software Group
IBM Malaysia

Risk – it's NOT a four simple letter word

- Successful organizations take a risk based approach to Information Security.
- Nothing can be 100% secure – but by knowing your current state, you can take a risk based approach.
- You can focus on implementing mitigating controls to address your most significant risks
- Successful organizations recognize risks, implement the appropriate mitigating controls and innovate / grow their business.
- **Security is no longer a constraint, but a business enabler**





Smarter Planet

The planet is becoming more...

- INSTRUMENTED,
- INTERCONNECTED and
- INTELLIGENT.

"We have seen more change in the last 10 years than in the previous 90."

Ad J. Scheepbouwer, CEO, KPN Telecom

New possibilities.
New complexities.
New risks.

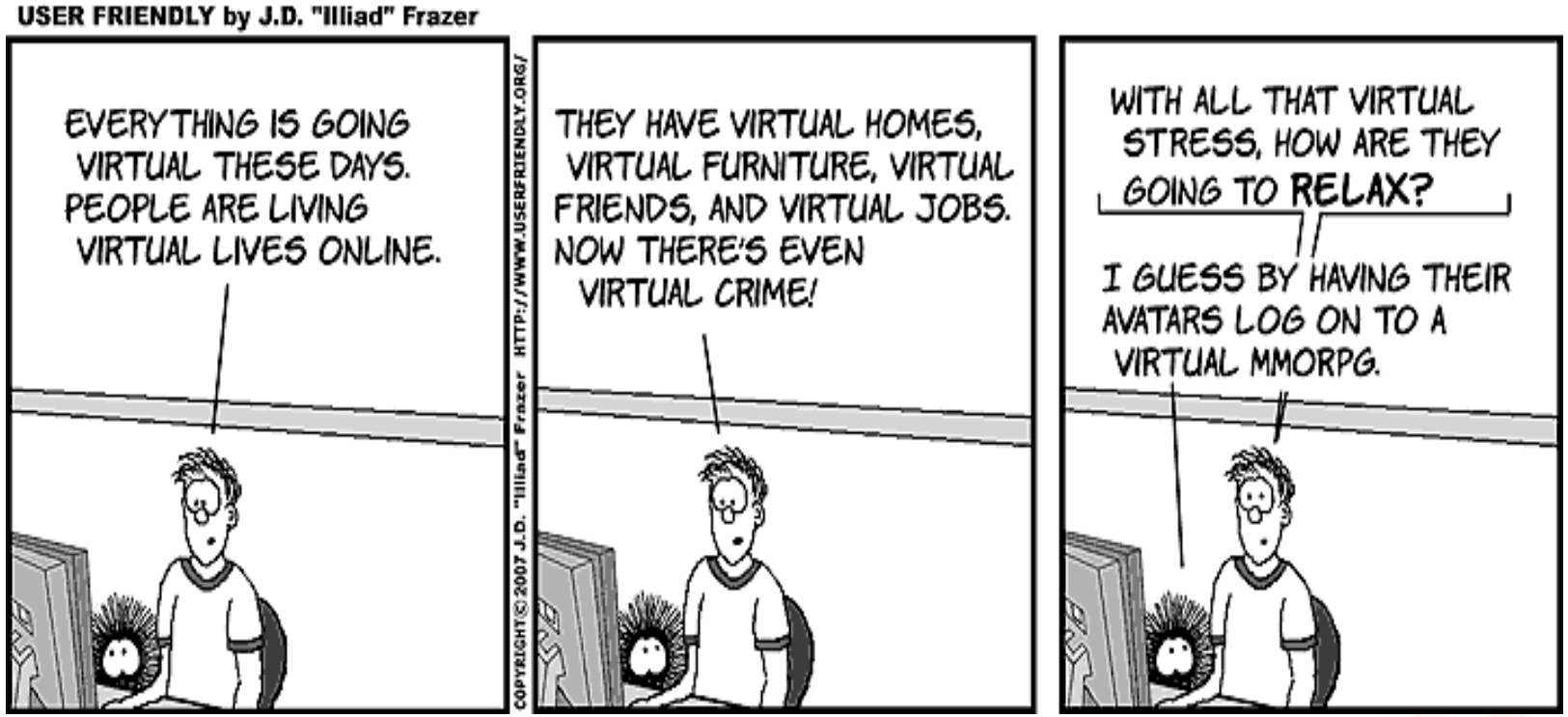
Critical infrastructure and application protection

Data privacy and identity controls

Data protection and recovery

Governance and policy management

The Virtual Reality



The Virtual Reality (continued)

itnews
FOR AUSTRALIAN BUSINESS

News | Technology | Business | Forums | Jobs

Reviews | Galleries | Events | Net Seminars | Whitepapers | Downloads | Newsletter | Videos

Home > News > Technology > Security > Cybercrime-as-a-service takes off

SECURITY

Cybercrime-as-a-service takes off

By Ry Crozier
Mar 12, 2009 11:37 AM
Tags: cybercrime | service | vasco | outsourcing | malware | trojan | toolkits

SHARE

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, the company's technical account manager, Vlado Vajdic, told delegates that cyber crime was becoming so business-like that online offerings of malicious code often included support and maintenance services.

Additionally, he said, cybercrime outsourcing would become a key trend in 2009.

"It was inevitable that services would be sold to people who bought the malware toolkits but didn't know how to configure them," Vajdic said.

"Not only can you buy configuration as a service now, you can have the malware operated for you, too. We saw evidence of that this year."

2 comments in this discussion

"This is not new, it's been a developing trend for the past couple of years, take a look at dancho danchev's blog..."

By Anon

Related Articles

- Laws to prosecute malware makers flagged
- Bit.ly hits back at Google

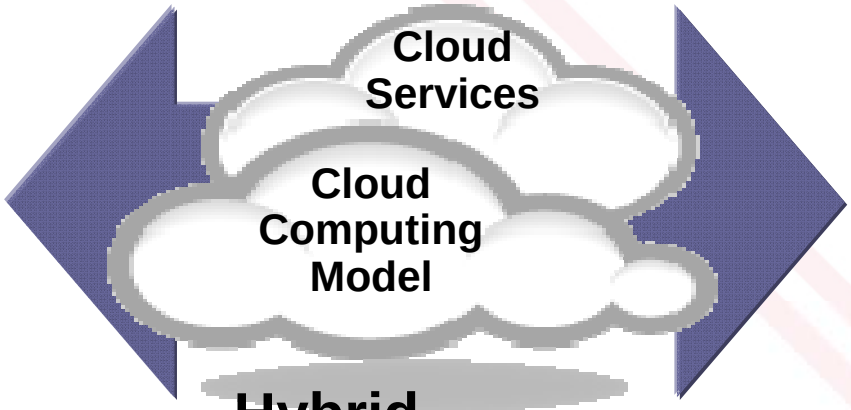
http://www.itnews.com.au/News/139682,cybercrime-as-a-service-takes-off.aspx

Cloud Computing Delivery Models

Flexible Delivery Models

Public …

- Service provider owned and managed
- Access by subscription
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis



Hybrid …

Access to client, partner network, and third party

Private …

- Privately owned and managed.
- Access limited to client and its partner network.
- Drives efficiency, standardization and best practices while retaining greater customization and control

…. Customization, efficiency, availability, resiliency, security and privacy

Recent Analyst Reports Confirm General Concerns

But also Highlight Security as a Potential Market Differentiator

- *"Securing your applications or data when they live in a cloud provider's infrastructure is a complicated issue because you **lack visibility and control** over how things are being done inside someone else's network."* Forrester, 5/09

- *"Large enterprises should generally **avoid placing sensitive information in public clouds**, but **concentrate on building internal cloud and hybrid cloud** capabilities in the near term."* Burton, 7/09

- *"Cloud approaches offer a **unique opportunity to shift a substantial burden for keeping up with threats to a provider** for whom security may well be part of the value proposition."* EMA, 2/09

- Gartner's 7/09 *"Hype Curve for Cloud Computing"* positions Cloud Security Concerns into the ***early phase*** (technology trigger, will raise), and gives it a time horizon of ***5-10 years***

- ***"Highly regulated or sensitive proprietary information should not be stored or processed in an external public cloud-based service*** *without appropriate visibility into the provider's technology and processes and/or the use of encryption and other security mechanisms to ensure the appropriate level of information protection."* Gartner 7/09

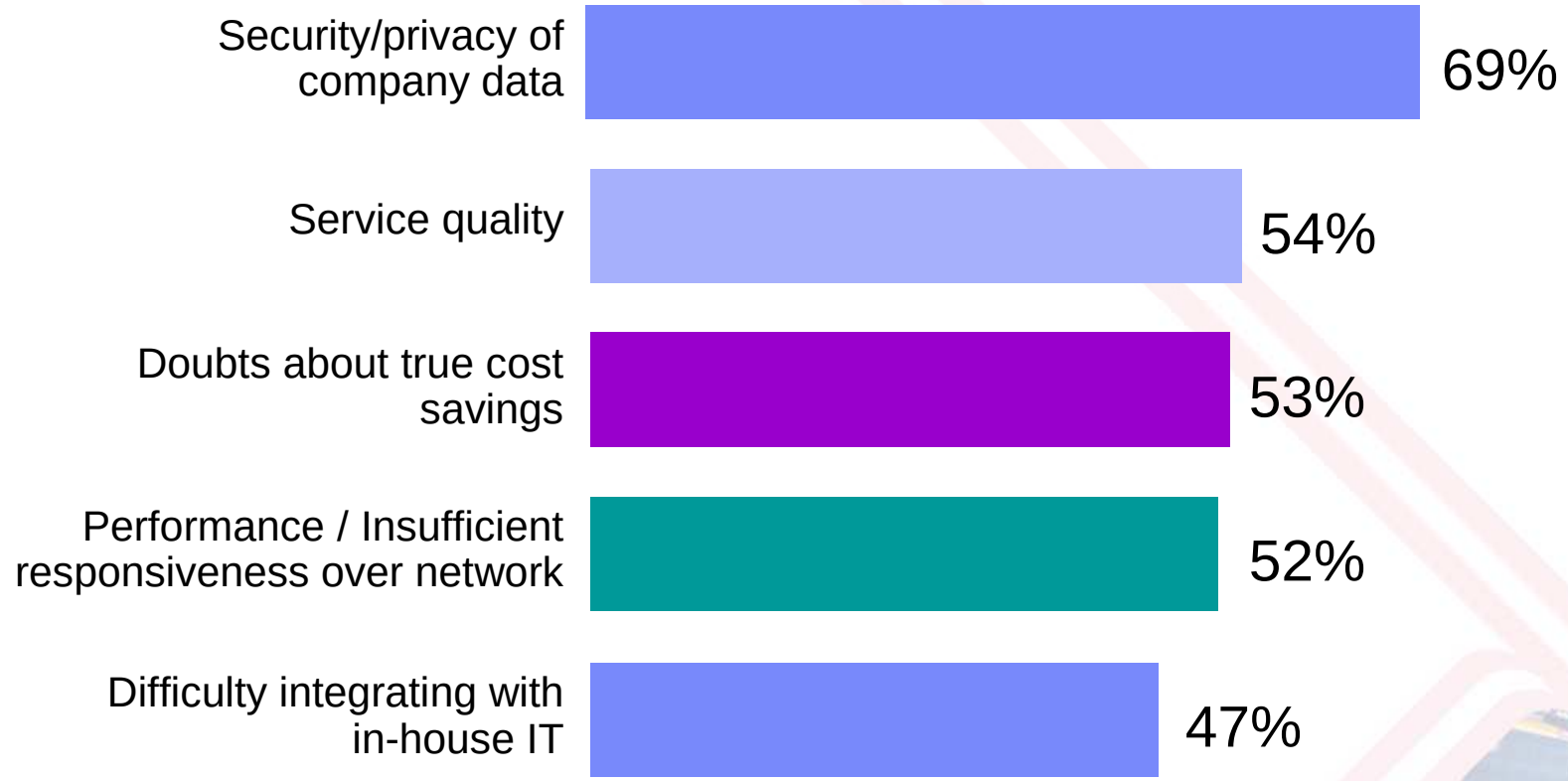
Specific Customer Concerns related to Security & Risk Management

Protection of intellectual property and **data**	30%
Ability to enforce regulatory or contractual obligations	21%
Unauthorized use of **data**	15%
Confidentiality of **data**	12%
Availability of **data**	9%
Integrity of **data**	8%
Ability to test or audit a provider's environment	6%
Other	3%

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey

Concerns about data security and privacy are the primary – but not the only - barriers to public cloud adoption

What, if anything, do you perceive as actual or potential barriers to acquiring public cloud services?



Percent rating the factor as a significant barrier (4 or 5)

Respondents could select multiple items

Source: IBM Market Insights, *Cloud Computing Research*, July 2009. n=1,090

Security Remains the Top Concern for Cloud Adoption

80%

Of enterprises consider security the #1 inhibitor to cloud adoptions

48%

Of enterprises are concerned about the reliability of clouds

33%

Of respondents are concerned with cloud interfering with their ability to comply with regulations

*"**How can we be assured that our data will not be leaked** and that the vendors have the technology and the governance to **control its employees from stealing** data?"*

*"**Security is the biggest concern.** I don't worry much about the other "-ities" – reliability, availability, etc."*

*"**I prefer internal cloud to IaaS. When the service is kept internally**, I am more comfortable with the security that it offers."*

Source: Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman)

Top Cloud Security Threats and Risks

- **Gartner: Top Risks (2008)**
- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

[Heiser 09]

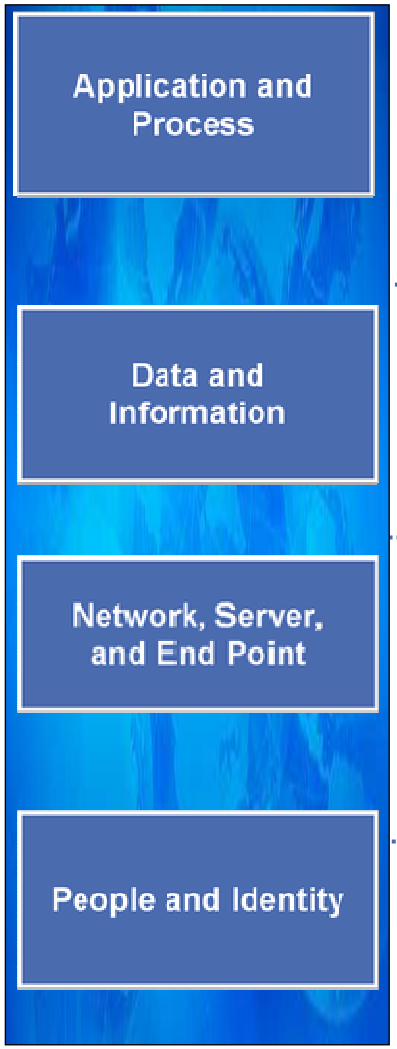
- **ENISA: Top Security Risks (2009)**
- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks
- Management interface compromise
- Data protection
- Insecure or incomplete data deletion
- Malicious insider

[ENISA 09/a]

- **CSA: Top Threats (2010)**
- Abuse and nefarious use of cloud
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

[CSA 10]

IBM X-Force Report 2010 Summary -- Attacks Continue Across all Security Domains



- Reported vulnerabilities are at an all time high, up **36%,** due to significant increases in public exploit releases and efforts by software vendors to identify and mitigate security vulnerabilities.
- **More than 55%** of all vulnerabilities disclosed are Web application vulnerabilities.
- **55%** of all vulnerabilities disclosed had no vendor-supplied patches available at the end of the 1st half of 2010.

- PDF attack activity continue to dominate the threat landscape. More than that, April 2010 had the most significant spike in PDF attack activity. Event activity for this month was almost **37%** higher than the average for the first half of 2010.
- The Zeus botnet toolkit continues to wreak havoc on organizations. Early 2010 saw the release of an updated version of the Zeus botnet kit, dubbed Zeus 2.0.
- Anonymous proxy websites continue to increase in volume, quadrupling since 2007.

- Advanced persistent threats are groups of attackers that target and successfully penetrate well defended networks.
- Attackers are continuing to find new ways to hide or mask their malicious traffic to evade security technologies, i.e. Javascript obfuscation.
- **35%** of virtualization vulnerabilities impact the hypervisor.
- **7.2%** of the Internet is considered “socially” unacceptable, unwanted, or flat out malicious.

- Brazil, the U.S., and India account for more than one fourth of worldwide spam.
- Majority of spam **(more than 90%)** is still classified as URL spam—spam messages that include URLs that a person clicks to view the spam contents.
- Amount of URL spam using well-known and trusted domain names continue to increase.
- The top spam domains have moved from China (.cn) to Russia (.ru).
- More than two thirds **(66.8%)** of all financial phishing targets are located in North America, the remaining **32%** are in Europe.

Categories of Cloud Computing Risks

Less Control

Many companies and governments are uncomfortable with the idea of their information located on systems they do not control. **Providers must offer a high degree of security transparency to help put customers at ease.**

Data Security

Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure. **Authentication and access technologies become increasingly important.**

Reliability

High availability will be a key concern. IT departments will worry about a loss of service should outages occur. **Mission critical applications may not run in the cloud without strong availability guarantees.**

Compliance

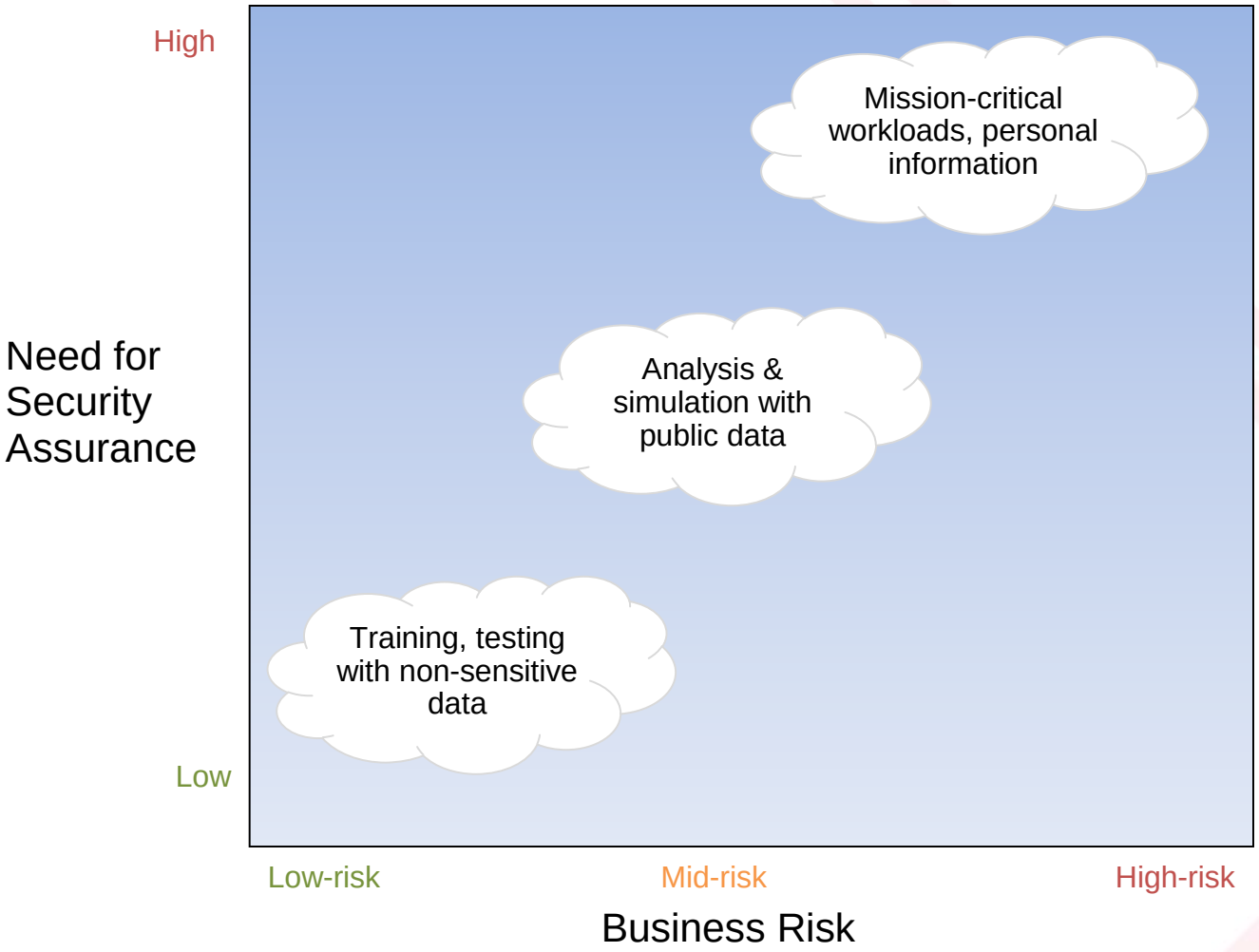
Complying with SOX, HIPAA and other regulations may prohibit the use of clouds for some applications. **Comprehensive auditing capabilities are essential.**

Security Management

Even the simplest of tasks may be behind layers of abstraction or performed by someone else. **Providers must supply easy controls to manage security settings for applications and runtime environments in the cloud**.

One-size does not fit-all:

Different cloud workloads have different risk profiles



Cloud 2.0+:

Tomorrow's high value / high risk workloads need:

- Quality of protection adapted to risk
- Direct visibility and control
- Significant level of assurance

Cloud 1.0+:

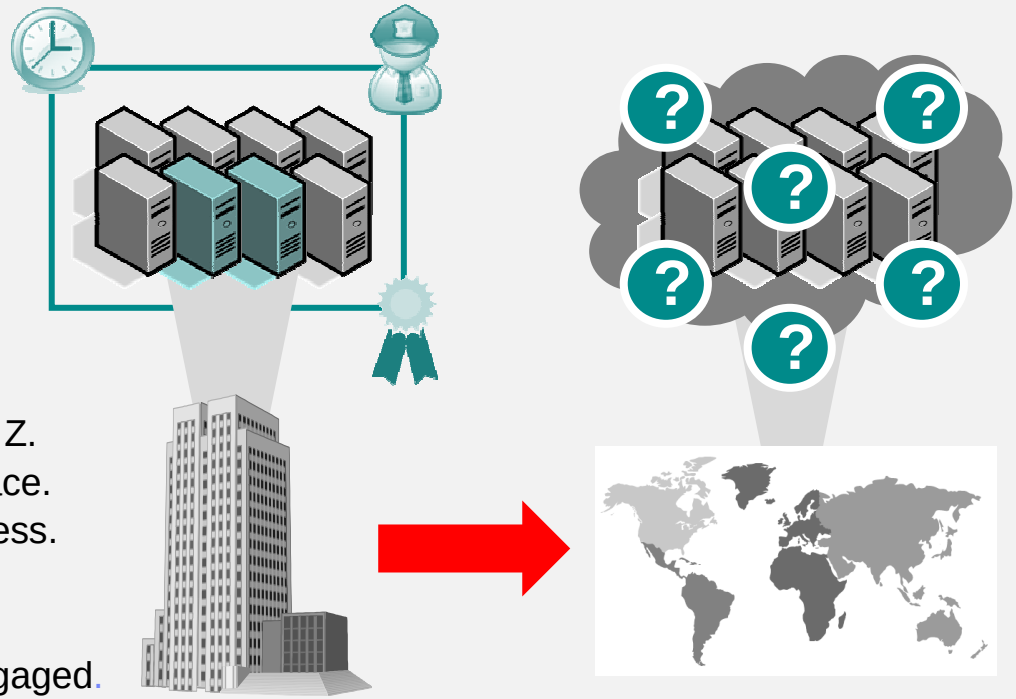
Today's clouds are primarily here:

- Lower risk workloads
- One-size-fits-all approach to data protection
- No significant assurance
- Price is key

Simple Cloud Security Consideration Example

Today's Data Center

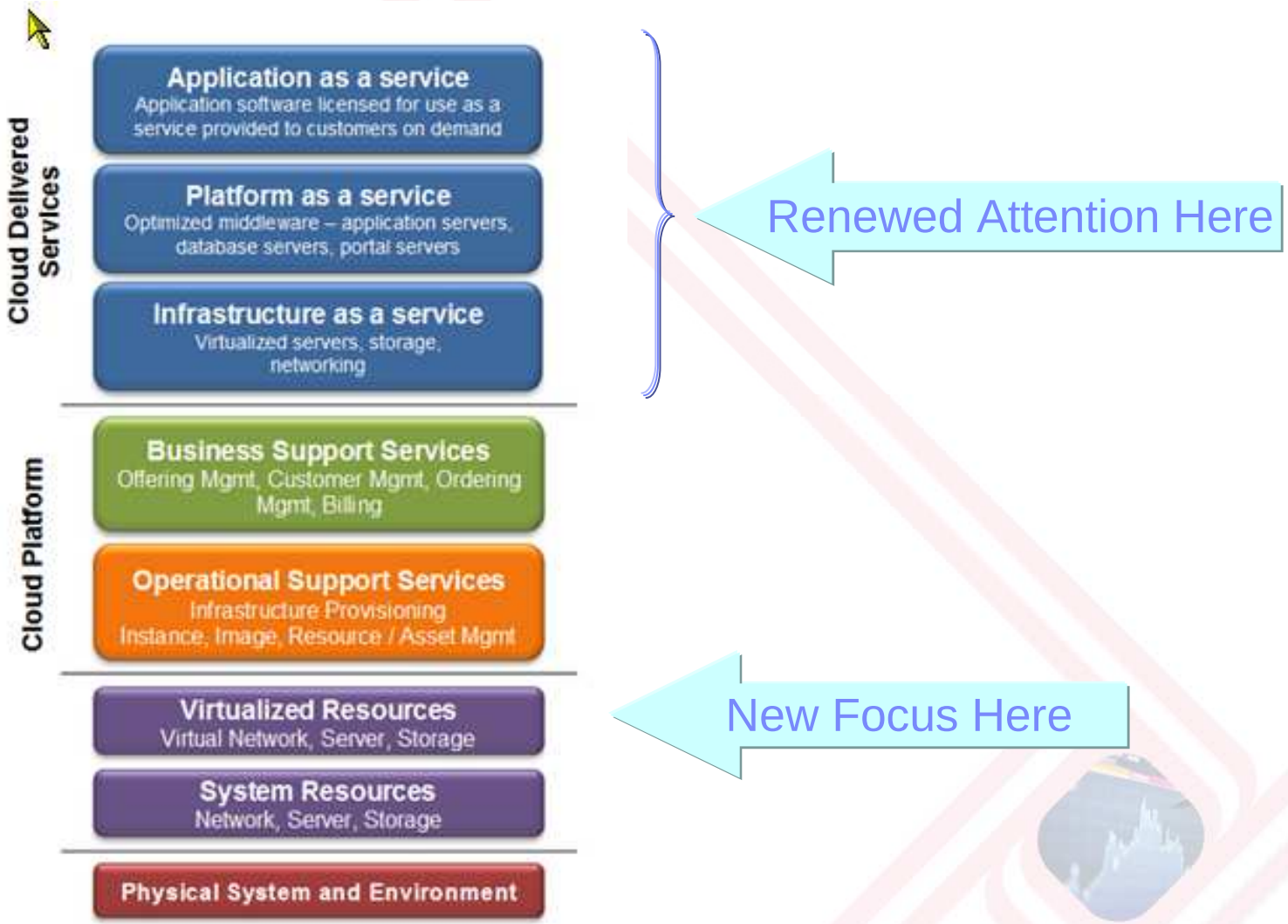
Tomorrow's Public Cloud



We Have Control
It's located at X.
It's stored in server's Y, Z.
We have backups in place.
Our admins control access.
Our uptime is sufficient.
The auditors are happy.
Our security team is engaged.

Who Has Control?
Where is it located?
Where is it stored?
Who backs it up?
Who has access?
How resilient is it?
How do auditors observe?
How does our security team engage?

Security and the Cloud Computing Stack



How we deliver Cloud Security

“We Believe the Cloud could be more secure than traditional Enterprises”

Security By Design

Security By Workload

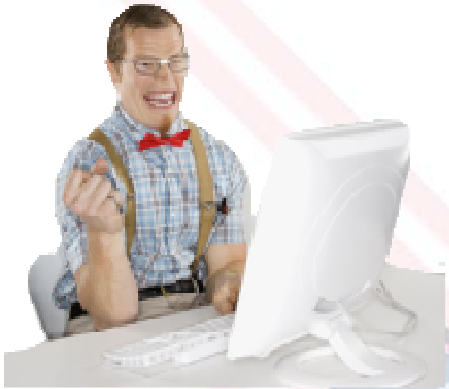
Security Efficiency

Security Innovation

Cloud Security depends on focusing security controls on specific Types of work

Healthcare

Public Services



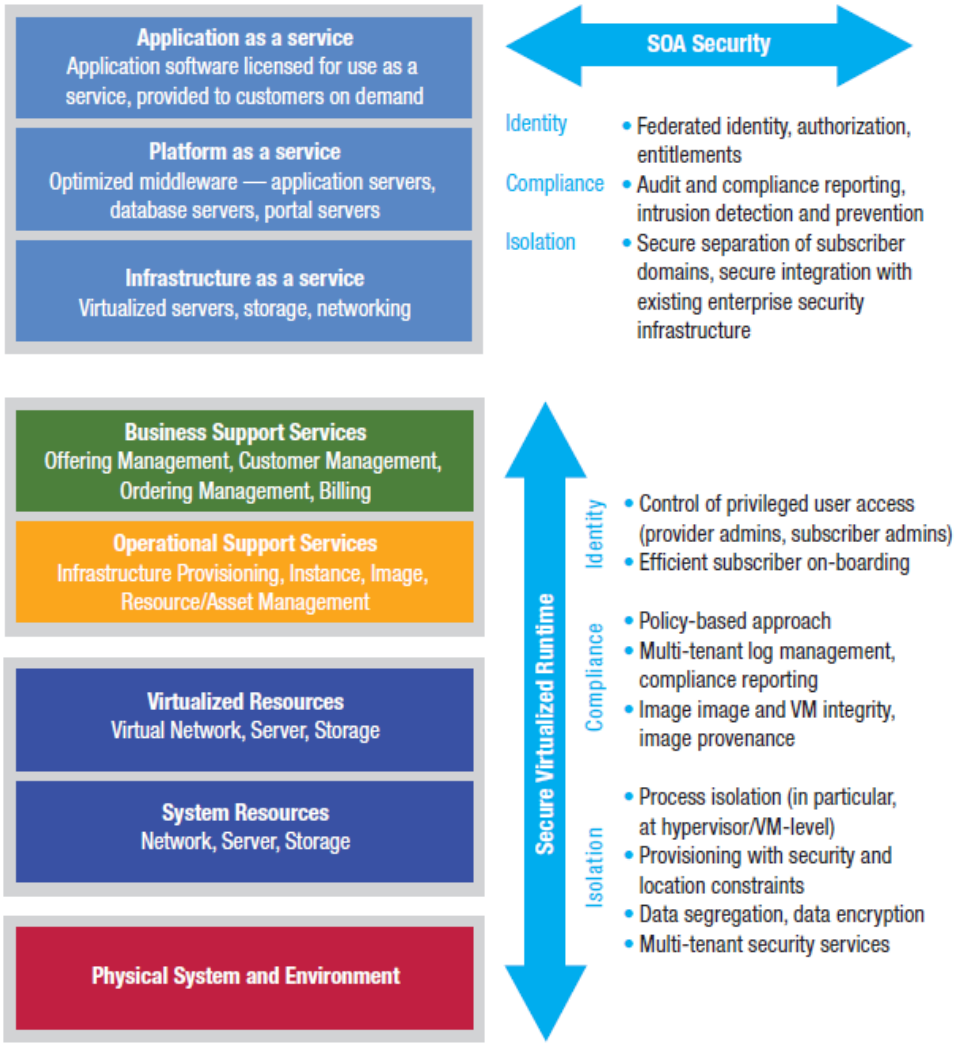
Financial

Investing in Security Innovation

IBM is researching how to apply emerging technology solutions to security in the cloud:

- Security for Social networking - allowing organizations to implement greater control and gain valuable insight into social networking activities.
- Advanced Security Analytics - leveraging IBM's advanced analytics capabilities to make sense of millions of security events.
- Security for Mobile Endpoints – Developing solutions that protect the cloud from emerging endpoints.

IBM Point of View: Security and Cloud Computing



SOA Security
+
Secure Virtualized Runtime
=
Cloud Security

Grid & Cloud Computing Security Requirements and Supporting Technologies


End User


Enterprise Administrator


IT Auditor


Application Developer


Cloud Provider

People and Identity

Privileged User Access
(centralized access and audit policies, directories)

Federated Identity Management
(single sign-on, identity provisioning technologies)

Privileged Account Management
(change control processes for privileged users)

Trusted Identity
(**protecting** their identities as constituents, employees, and consumers)

Data and Information

Data Segregation
(encryption, network segmentation, Hardware / OS / App / Database isolation)

Data Recovery
(centralized backups, remote storage)

Data Redaction and Termination
(secure removal processes for customer data and metadata)

Data Leakage Prevention
(DLP technologies for data in motion and data at rest)

Application and Process

Compliance and Auditing
(audit policy creation, log generation and management)

Investigative Support
(audit retention, search, and correlation)

Policy Management
(unified security, governance, and policy enforcement)

Secure Provisioning
(image management, hardening, cohabitation policies)

Application Testing
(vulnerability assessment, fuzzing, app scanning, automated code reviews)

Network, Server, and Endpoint

Server Security
(trusted computing, auditing, access control)

Network Security
(Firewall, IPS, VLAN)

Virtualization Security
(VM Segmentation, Virtual Appliances, Integrated Hypervisor Security)

Browser Security
(ssl, memory protection, multi-level security, anti-malware)

Patch Management
(assessment, prioritization, scheduling, and application)

Physical Infrastructure

Data Location
(cloud data centers)

Disaster Recovery
(highly resilient clouds)

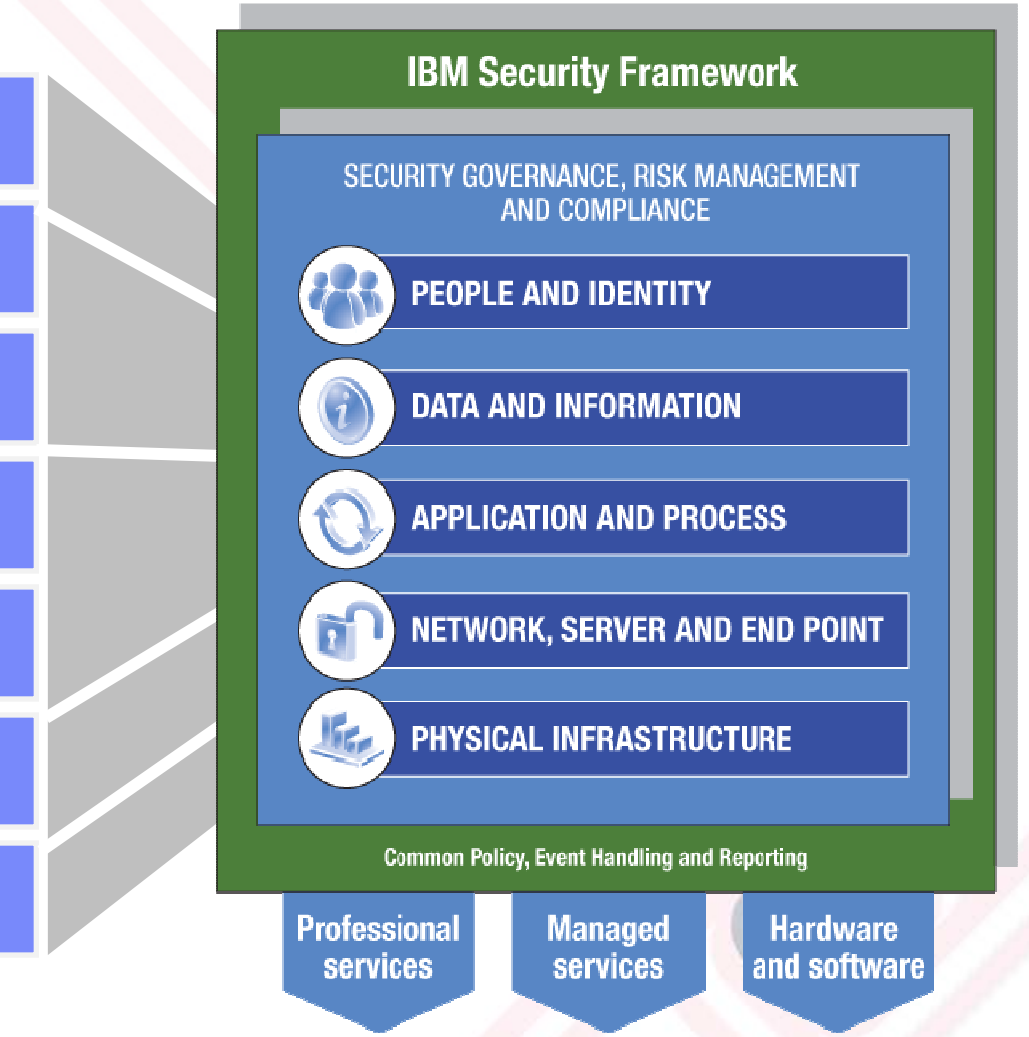
Cloud Availability
(multiple cloud centers)

IT moves to writing SLAs!

Gartner Reports on Security Risks of Cloud Computing

…that map directly to the IBM Security Framework.

- Privileged User Access
- Data Segregation
- Data Recovery
- Investigative Support
- Regulatory Compliance
- Data Location
- Disaster Recovery



Gartner: Assessing the Security Risks of Cloud Computing, June 2008

Thank you!