COMPUTERWORLD SNIA

SNW

Transforming the Information Infrastructure: Build, Manage, Optimize.

FALL 2011

Security, Privacy, and Regulations in the Cloud

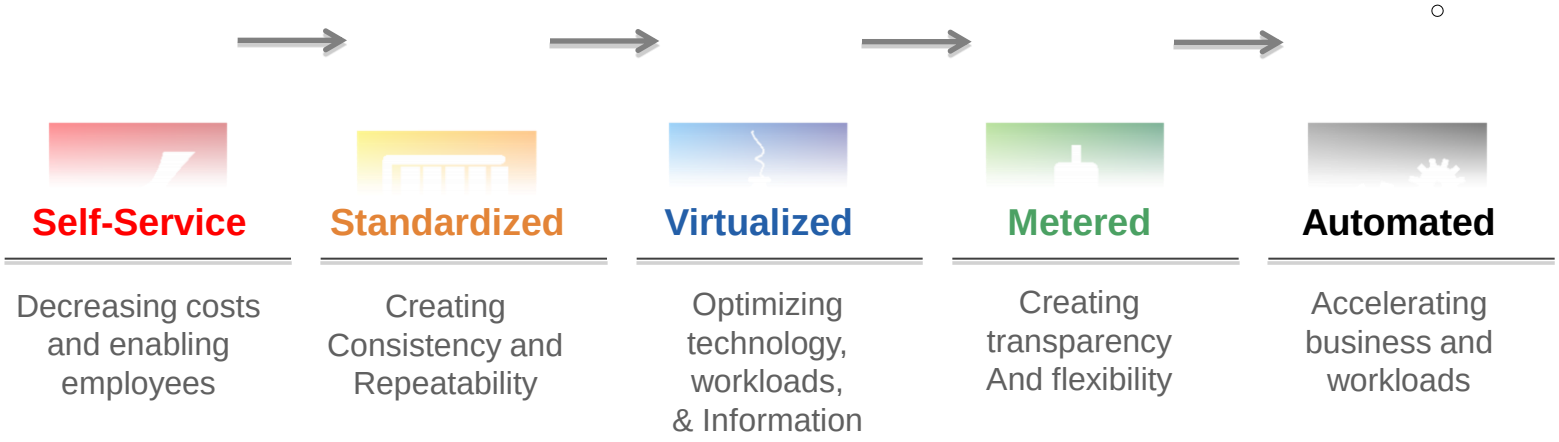
Marne E. Gordan
Regulatory Analyst
Corporate Security Strategy Group
IBM

Agenda

- Threat Landscape
- Security
- Privacy
- Regulations
- Successfully Managing the Cloud
- Summing Up
- Q & A

IBM's perspective on Cloud Computing…

"Cloud computing represents a new model for delivering and consuming business services, resulting in significant economies of scale of, greater business agility and improved cost controls."



But There Were High Profile Breaches in 2011

90% of Security Professionals discussed High Profile breaches with their Management

23% ACTED on those discussions

"Breaches that occurred in the first half of 2011 have changed the rules of security by exposing high profile companies like RSA, Sony, Lockheed Martin and numerous others," said Tom Murphy, chief strategy officer, Bit9

Cloud computing impacts the implementation of security in fundamentally new ways

Security and Privacy Domains	To cloud
People and Identity	Multiple Logins, Numerous Roles
Data and Information	Multi-tenancy, Shared Resources
Application and Process	External Facing, Quick Provisioning
Network, Server and Endpoint	Virtualization, Reduced Access
Physical Infrastructure	Provider Controlled, Lack of Visibility
Governance, Risk and Compliance	Audit Silos, Logging Difficulties

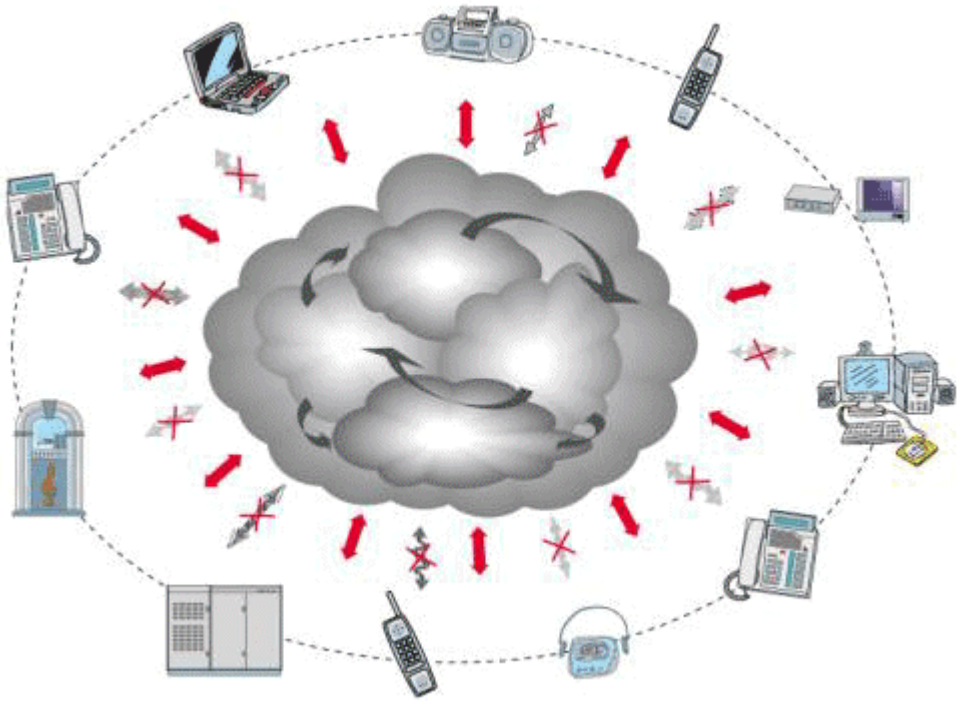
In a cloud environment, access expands, responsibilities change, control shifts, and the speed of provisioning resources and applications increases - **greatly affecting all aspects of IT security**.

Security as a Barrier to Successful Cloud Deployment

Security concerns surrounding cloud computing continue to be a common inhibitor of widespread usage.

To gain the trust of organizations, cloud-based services must deliver security and privacy expectations that meet or exceed what is available in traditional IT environments.

Cloud Security



43% of current cloud users **reported a security incident** in the past 12 months

Cloud Threat Landscape

2010-2011 Breach Statistics (ITRC)

Cloud Breaches since Jan 2010

130	Breaches
9.5	Total Records In Millions

Jan - 2011 — Apr 5- 2011

37%	# of Malicious Attacks up
+17%	Increase over all of 2010

Protection of Lost Sensitive Data

1	Percent of lost data secured by encryption
5	Percent of lost data protected by Password

Information Week Analytics

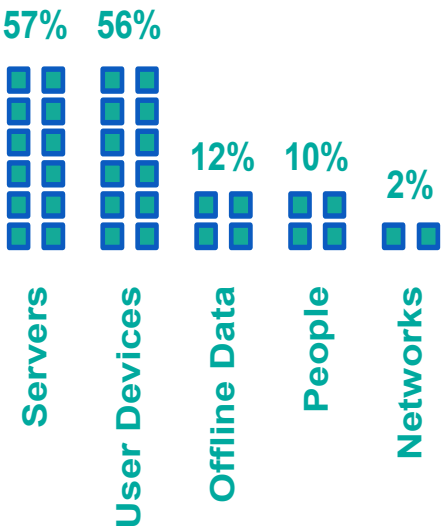
Protection of Lost Sensitive Data

55%	Lack of interoperability with other productivity or network software.
47%	Cost of buying Encryption technology.
34%	Lack of management sponsorship or organizational imperative.

Verizon 2011 Security Survey

92%	Breaches Involving External persons
17%	Breaches Involving Internal persons

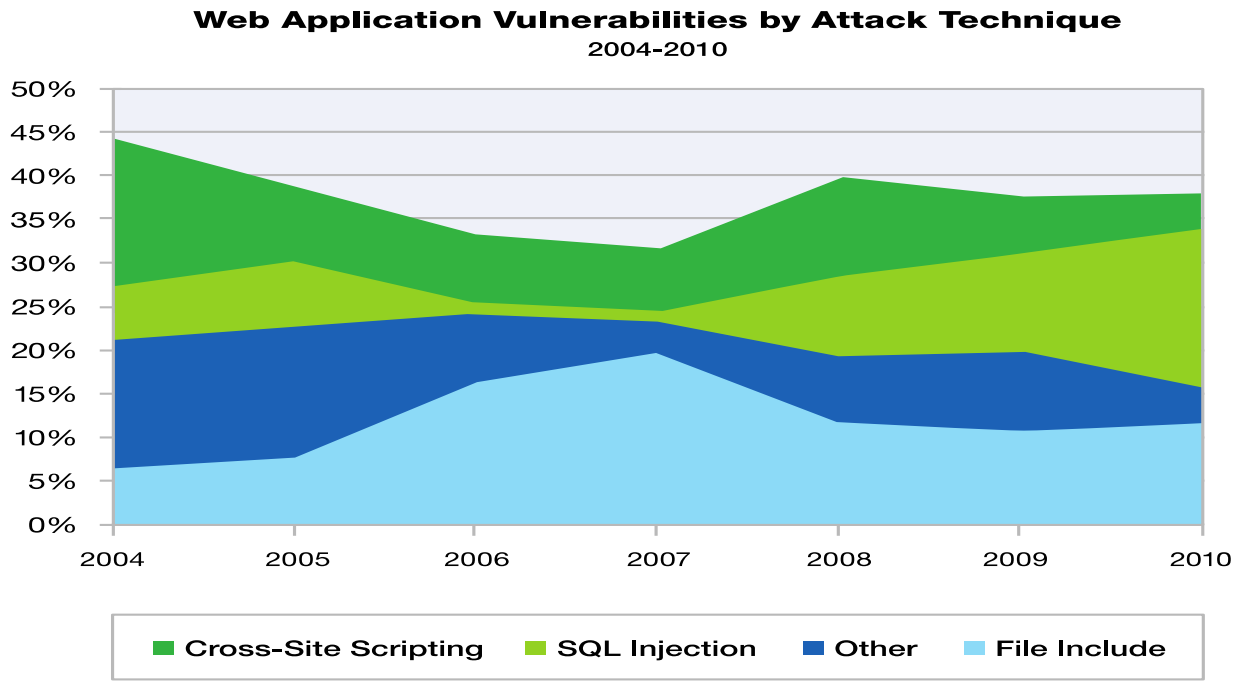
Affected Assets by Breach



Threats to Cloud Adoption

49% Percent of vulnerabilities disclosed in 2010

44% Percent of 2010 vulnerabilities without patches.



IBM X Force Report

Do These Sound Familiar ??

SQL Injections are code injections which exploit vulnerabilities in relational databases. They represent one of the more common vulnerabilities to enterprises.

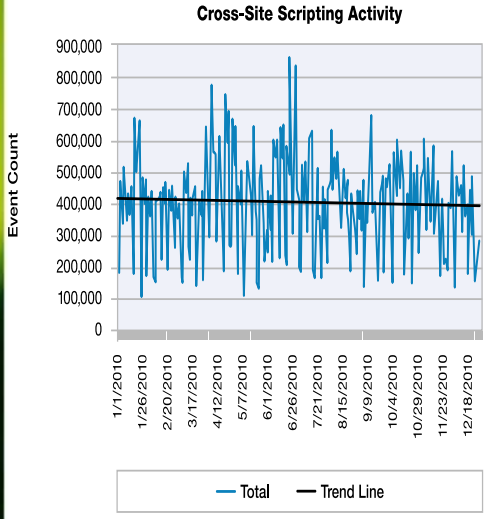


Figure 6: Cross-Site Scripting Activity

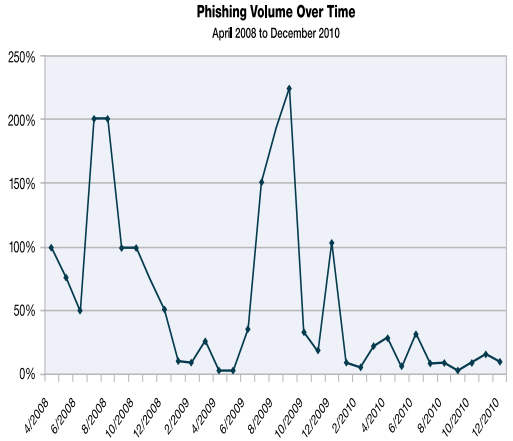


Figure 36: Phishing Volume Over Time – April 2008 to December 2010

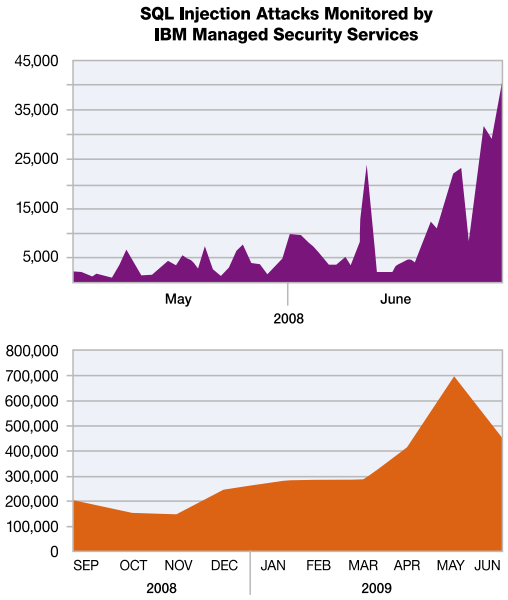
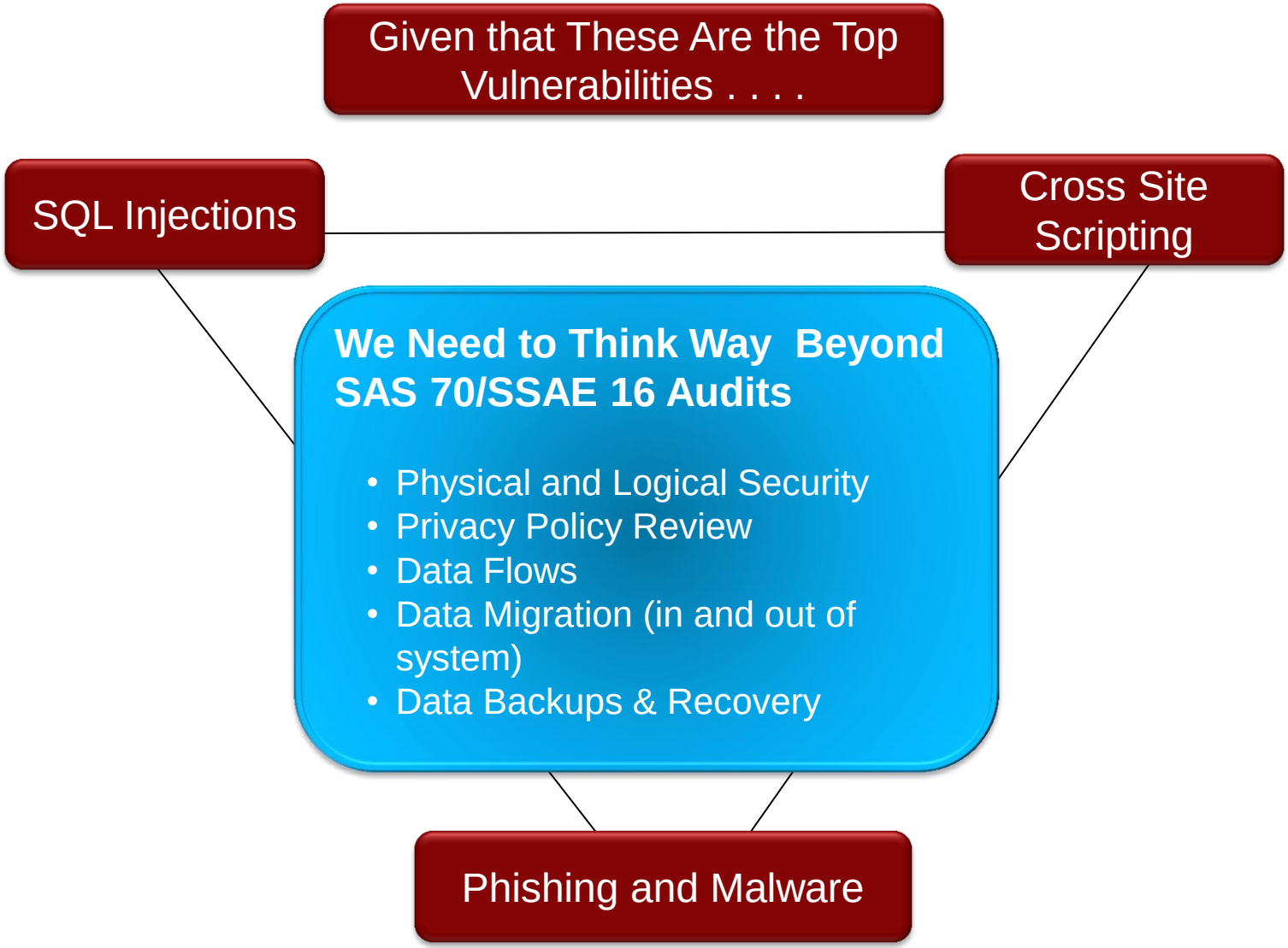


Figure 2: SQL Injection Attacks Monitored by IBM Managed Security Services

Cross Site Scripting enables attackers to inject client side script into webpages. This occurs by executing codes.

Programming designed to disrupt, deny access or gather information that leads to loss of information or exploitation of weakness.

Information Security:
So Much More Than Certification

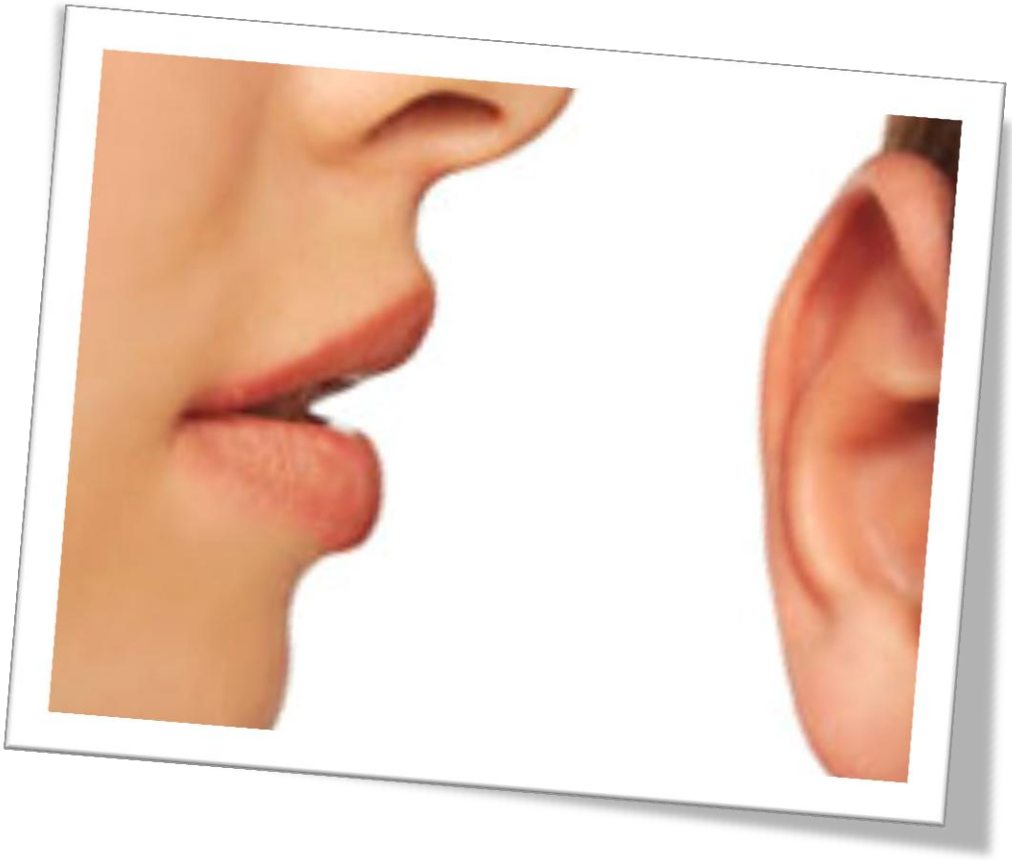


In Short . . .

In the cloud, everything new is old again

- Threats and vulnerabilities that are contained in traditional data centers are successful in the cloud
- Why?
  - We have placed historically vulnerable vectors (example - applications)
  - In an emerging technology
  - Creating a “sweet spot” for attackers
  - Leading to accidental or easily executed malicious exposures

Privacy Issues in the Cloud



B2C Privacy Policy Considerations

***Information about our customers is an important part of our business, and we are not in the business of selling it to others.** We share customer information only as described below and with subsidiaries XYZ.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

Affiliated Businesses We Do Not Control: We work closely with affiliated businesses. In some cases, such as Marketplace sellers, these businesses operate stores at XYZ.com or sell offerings to you at XYZ.com. In other cases, we operate stores, provide services, or sell product lines jointly with these businesses. Click here for some examples of co-branded and joint offerings. **You can tell when a third party is involved in your transactions, and we share customer information related to those transactions with that third party**

.

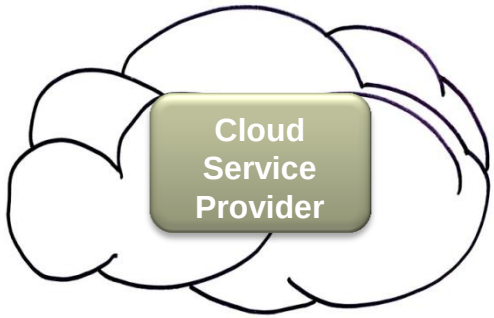
Third-Party Service Providers: We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. **They have access to personal information needed to perform their functions, but may not use it for other purposes.**

*taken from a privacy statement posted online 09/06/2011

Consumer

Consumer and Organization agree not to:
- Sell
- Share
- Allow Open Access

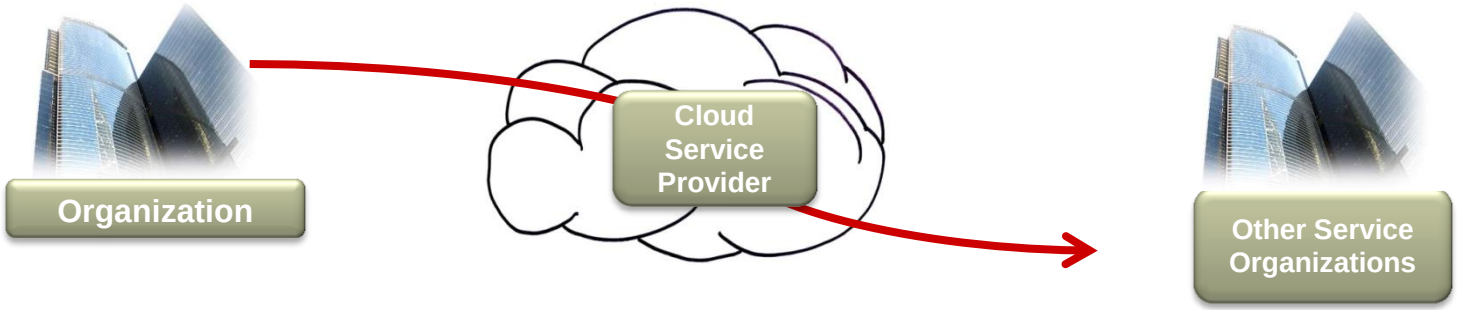
Organization



Do Organization and Cloud Provider agree not to:
- Sell
- Share
- Allow Open Access

Defining the 3rd Party Relationship

What is the Cloud Provider's relationship with the Organization's data?



As the organization engages 3rd parties, questions and considerations to discuss are:

- Do they have the right to resell data?
- Do they have the right to share info? With who?
- Who is allowed access to info?
- Do they engage with other 3rd parties to provide services?
- What are the cloud provider's privacy policies?

Information Transfer Considerations

Does the target workload include the organization's intellectual property or trade secrets?

Has the organization discussed with the cloud provider:

- How is confidential information handled?
- How is access limited?
- Is the principle of least privilege applied?
- In a multi-tenancy deployment, might this information be exposed to individuals outside the organization?

Privileged Communication Expectations

Does the target workload include any communication which must remain confidential?

Attorney

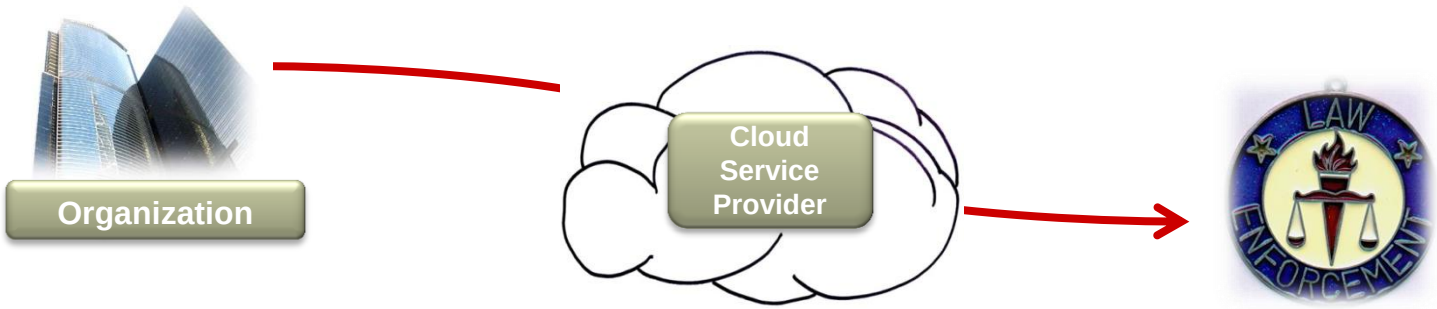
Client

The organization may want to consider:

- Is this the right workload for a cloud deployment?
- Is this an IT decision? If so, has a business manager reviewed and/or approved the decision?
- Are there chain of custody issues that the organization will be required to demonstrate or prove?
- Can the data be encrypted prior to transfer in order to preserve privilege?

Expectation of Privacy Considerations

Can personal property/communications be co-mingled with the target workload?



Depending upon workload, the organization should consider the impact of personal property/communications and/or inappropriate content being introduced into the target :

- Who owns the data?
- Who has the right to look at it?
- What is the role of the service provider?
- How will they respond to requests from law enforcement?
- What might the organization's exposure be in a multi-tenancy environment, relative to tenants that are subjects of investigation?

In Essence . . .

Cloud computing creates multiple opportunities for unplanned disclosures and exposures

- The organization should
  - Review data classification schemes
  - Review data transfers to 3rd parties
  - Ensure that LOB managers and IT understand and agree on cloud deployments

What is the Regulatory Perspective ??

No Shortage of InfoSec/Privacy Mandates . . .

US Federal

HIPAA
Health Insurance Portability & Accountability Act

HITECH Act

GLBA
Gramm-Leach-Bliley
Compliant

FERPA
Family Educational Rights and Privacy

FRCP

DIGITAL DUE PROCESS
Updating the Electronic Communications Privacy Act

International Privacy Law

US State PII Protections

ISO 27001
REGISTERED FIRM

PCI DSS COMPLIANT

COBIT 5:
The Framework

Industry/Contractual/Voluntary

White House Cyber Security Agenda

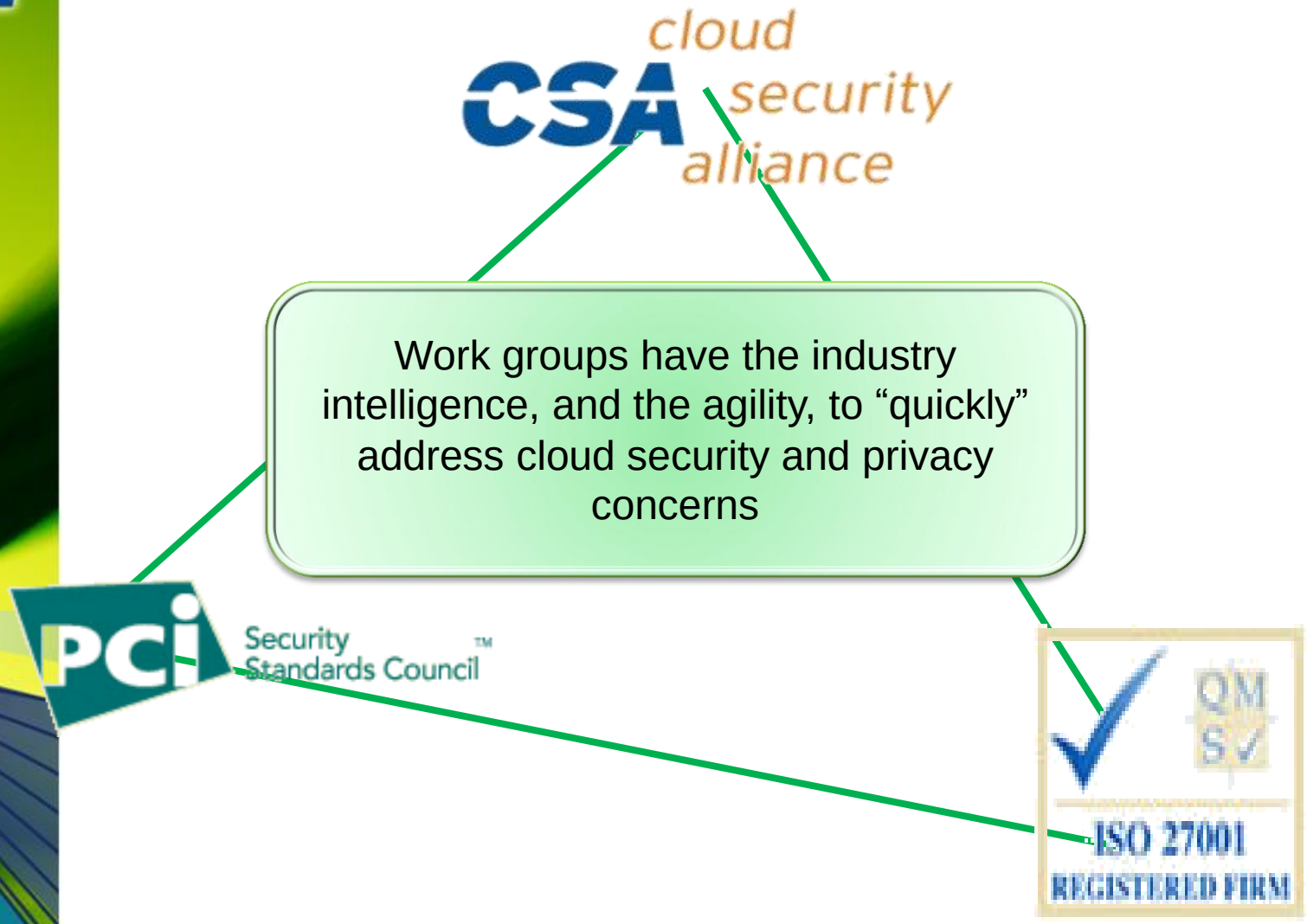
DHS Consolidation and FISMA Reform

Data Privacy (PII)

Emerging Technologies and Cloud Computing

End Game: Improve Data Protection

Industry Work Groups Take the Lead



In General . . .

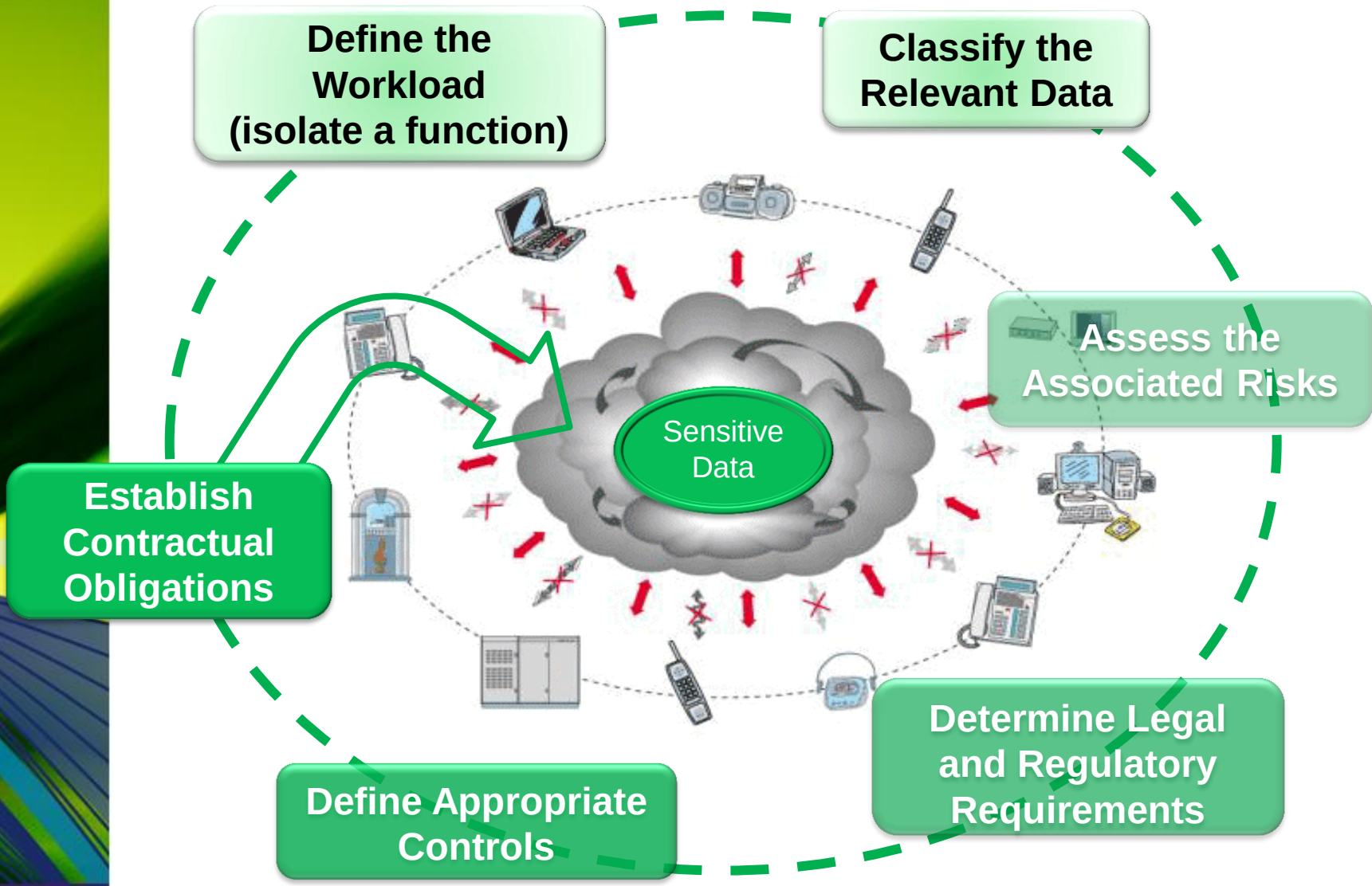
Cloud technology, in itself, is not likely to be regulated

- It is not practical to regulate a computing platform
- There is no precedent
- There is no predominant supervisory authority or jurisdiction

- Industry regulation may establish guidance for cloud computing in general, or requirements for specific types of deployments
- The industry work groups will continue to lead for the foreseeable future

Successfully Managing the Cloud

Success Through "Data Centricity"



One Size Does NOT fit all!

Some providers will state that all workloads are appropriate to a single purpose cloud offering – this is disingenuous. Successful adoption of cloud technology depends on a workload driven approach to addressing cloud needs.

There are Multiple Delivery Models for Clouds

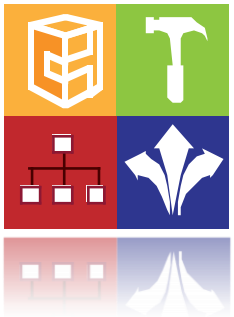
Hybrid Cloud

Private Cloud	Managed Private Cloud	Hosted Private Cloud	Shared Cloud Services	Public Cloud Services
				
Your Equipment Your Resources	Your Equipment Someone Else's resources	Trusted 3rd Parties Equipment and Resources Dedicated Hardware	Trusted 3rd Party Shared Services, Software	Trusted 3rd Party Shared Infrastructure

Why Workload Focus Matters

	HEALTHCARE	Collaboration
Risks	■ Data Breach ■ Regulatory Impacts ■ Unauthorized Access ■ Brand Damage ■ Auditability ■ Class Action suits	■ Unauthorized Access ■ Data Leakage ■ Malware ■ Legal Hold ■ e-Discovery
Considerations	■ Access Management ■ Identity Management ■ Data Encryption ■ Audit ■ Forensics ■ Data Leakage Prevention	■ Access Management ■ Anti-Malware ■ Data Encryption ■ e-Discovery ■ Anti-Spam ■ Archive ■ Data Leakage Prevention

Fundamentals and Pragmatic Security



	Secure By Design	Service Enabled	Innovation Empowered
What?	Focus on building Security into the fabric of the cloud	Enabling security through services and Interfaces	Leveraging innovations to empower security
Why?	Failure to build security into foundation often results in security and customer satisfaction issues.	Security is hard and can be expensive especially in a distributed environment like cloud computing	The cloud is evolving at a Geometric rate, customers need tomorrow solutions today.

“The Cloud has the Potential to be more secure than traditional environments”

Data Isolation

Enterprises adopt cloud technologies in precise ways, as a results they don’t lump all their valuables in one place

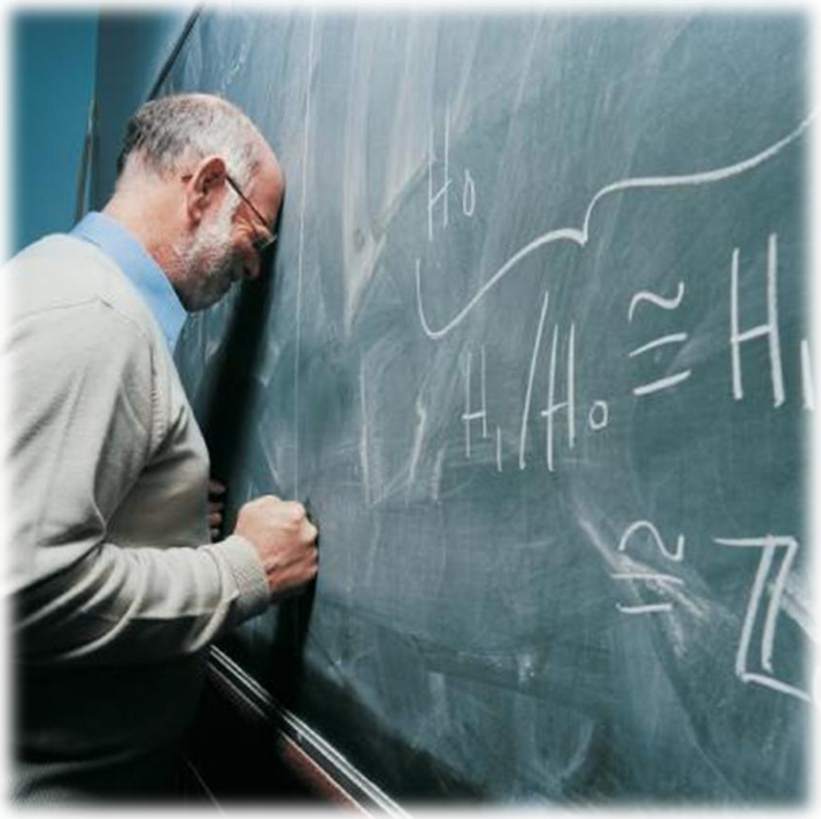
Resource Availability

Clouds Offer increased availability and the ability to do more with less, and providers see as competitive advantage

Skills Availability

Public Clouds and Security Services allows organizations to compensate for skill deficiencies

Summing Up



Easy To Say . . .

1. Define a Workload
2. Identify the Risks
3. Establish Controls
4. Choose a Cloud Deployment
5. Select a Vendor/Partner
6. Etc.
7. . . . . .

A Little Harder to Put into Practice

Secure by Design for Cloud Computing

Cloud computing requires organization break down the traditional cloud boundaries and look beyond silos of security, for organizations to successfully adopt cloud based technologies they need to build security into their cloud intiiatives very fabric. The secure by design approach for cloud computing, focuses on building a foundation for the cloud which considers the dynamic nature of cloud adoption as well as the various delivery and deployment options to help build a secure cloud environment, and enable the management of that environment.

Challenges

Access & Identity

The dynamic nature of cloud computing makes managing access & identity difficult.

Data Loss

Elasticity and mobility of data makes managing information in the cloud more diffcult.

Lock-In

Poor design choices can result in vendor lock-in issues, as well as issues integrating clouds into existing security paradigms.

Management

Failure to consider management requirements at the onset can result in inability to integrate or increased operational costs.

Audit

Elasticity, mobility and vendor policies can result in increased audit challenges and an inability to address regulatory requirements.

Design

Plan
Identify foundational controls, cloud workload and risk appetite and security policies.

Define
Determine deployment and delivery models as well as unique workload security needs.

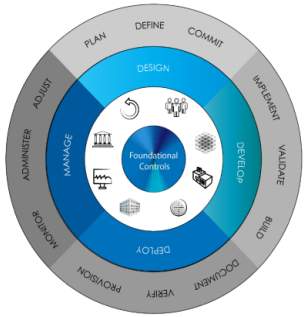
Commit
Establish buy in and build consensus between business and IT. Document decisions, requirements and foundational controls.

Develop

Implement
Create architecture, and assemble the cloud components and management controls.

Validate
Verify cloud conforms with defined security parameters and requirements.

Build
Assemble and label finalized components with pre-configured security attributes.



Opportunities

Data Awareness

The very nature of how organizations adopt cloud computing results in improved data awareness and security understanding

Extensibility

Cloud technologies allow organizations to compensate for security deficiencies via security services

Resilliency

Cloud computing allows organizations to build highly resilient systems which can be rapidly deployed.

Financial Value

Cloud based security allows organizations to invest in a broader set of security options at a lowe cost, and at a increased time to market.

Transparency

The isolated nature of the cloud allows organizations to better understand access and identity needs as well as data relevance.

Manage

Monitor
Implement active event and log monitoring of all cloud instances.

Administer
Govern cloud instances, perform regular audit and assessment of security policies and conditions.

Adjust
Adjust cloud configuration to ensure alignment with foundational controls, workload requirements and organizational guidelines.

Deploy

Document
Document and manage cloud instances communicate security requirements.

Verify
Validate pre-production instances against security requirements, ensure compliance with design.

Provision
Deliver solution to target environment, ensure compliance with security policies.

Workload is Key

- Public cloud offerings are good – but not for every function
- Hybrid and private clouds offer increased benefits
- A data centric security model sets up
  - Workloads
  - Risks
  - Requirements
  - Controls
- Workload sets the stage for selecting the correct deployment and provider

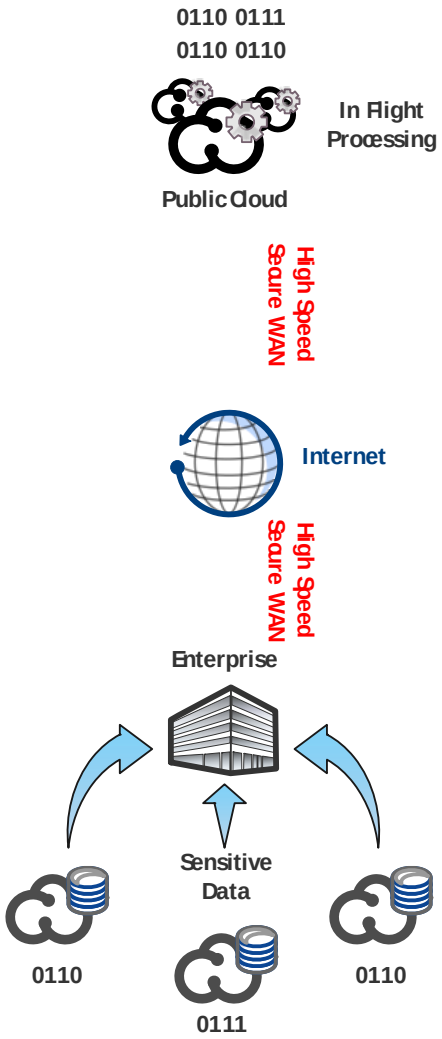
We've Seen These Risks and Threats Before

- Cloud computing holds all of the risks of a typical web hosting shared services arrangement.
- Emerging technologies plus largely undefined threat landscapes create opportunities for opportunists
- Attackers are "going back to basics" – using old attacks on new technologies
- We need to go back to security fundamentals to protect our cloud deployments

Cloud and Sensitive Data Challenges

Lessons learned from early adopters:

- Leverage Data in Transit to protect Sensitive Data
- Implement a Secure by Design Methodology when adopting Cloud
- Distribution of Data/Data Processing is critical to protecting information
- Leverage Virtual Desktop Technology to minimize leakage
- Implement Active Monitoring



Select the Right Provider

- Avoid take-it-or-leave-it agreements with standard, non-negotiable terms.
- Ensure that your organization's data is not inadvertently mingled with that of any other client (especially a competitor).
- Ascertain the provider's data segregation procedures:
  - Ensure that no one other than your organization has access to the data, even in a multi-tenant shared- hosting environment
  - Determine how frequently the provider monitors its environment to confirm that data is properly segregated?
- If the cloud computing service provider is not willing to negotiate a contract, then the provider may not be worth the supposed cost savings.

IBM Cloud Security Guidance

Based on cross-IBM research and customer interaction on cloud security

Highlights a series of best practice controls that should be implemented

Broken into 7 critical infrastructure components:

- Building a Security Program
- Confidential Data Protection
- Implementing Strong Access and Identity
- Application Provisioning and De-provisioning
- Governance Audit Management
- Vulnerability Management
- Testing and Validation


IBM

Redpaper

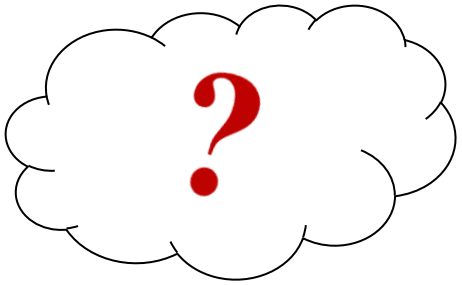
Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

Introduction to cloud computing

Q & A

- Contact Information
  - Marne E. Gordan
  - Regulatory Analyst
  - IBM Corporate Security Strategy Group
  - megordan@us.ibm.com
  - +1 703 960 9536




COMPUTERWORLD
SNIA
SNW


Thank
You


IBM

Disclaimer

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

IBM Global Security Reach

IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

COMPUTERWORLD SNIA

SNW

Transforming the Information Infrastructure: Build, Manage, Optimize.

FALL 2011