Morgan Lewis

Outsourcing in a Web-Based, Mobile World

February 23, 2012

Barbara Melby | Chris Kalnik | Peter Watt-Morse

Introduction

Please note that any advice contained in this presentation is not intended or written to be used, and should not be used, as legal advice.

Participants

Barbara Melby
partner
Morgan Lewis
Phone: 215.963.5053
Email: bmelby@morganlewis.com

Peter Watt-Morse
partner
Morgan Lewis
Phone: 412.560.3320
Email: pwatt-morse@morganlewis.com

Chris Kalnik
Partner
ISG
Phone: 845.266.8296
Email: chris.kalnik@isg-one.com

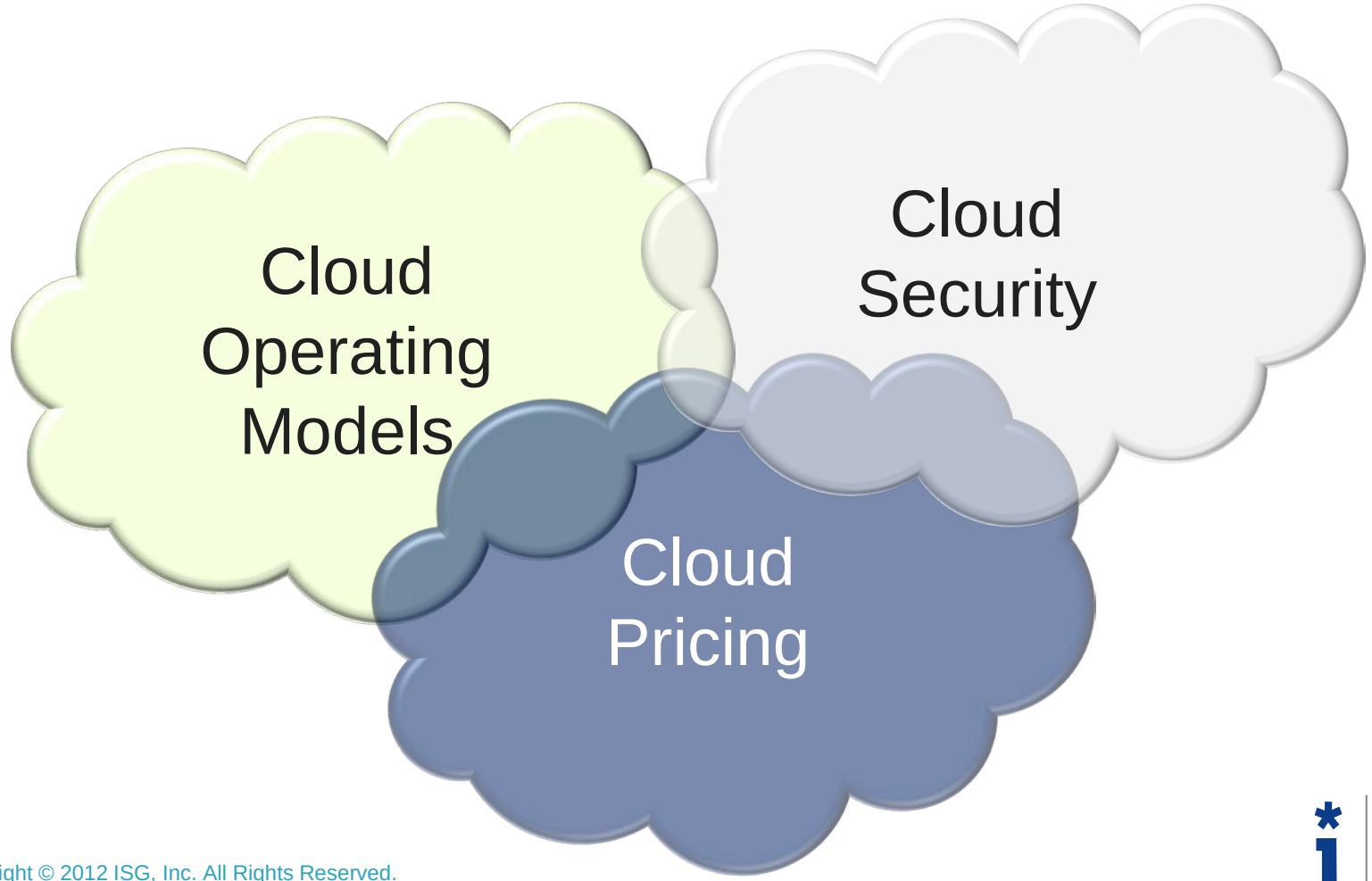
Agenda

- Introduction
- Outsourcing and the Cloud: An Industry View
- Managing Mobile Devices in the Workplace, Including a Look at Social Media Issues
- Reevaluating Security Requirements in a Web-Based World

Outsourcing and the Cloud: An Industry View

Chris Kalnik

Agenda



ISG
INFORMATION
SERVICES
GROUP

Let’s Agree on Common Definitions

Institute of Standards and Technology defines “Cloud Computing” as follows:

- A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- This cloud model promotes availability and is composed of essential characteristics, service models, and deployment models.

Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Service Models

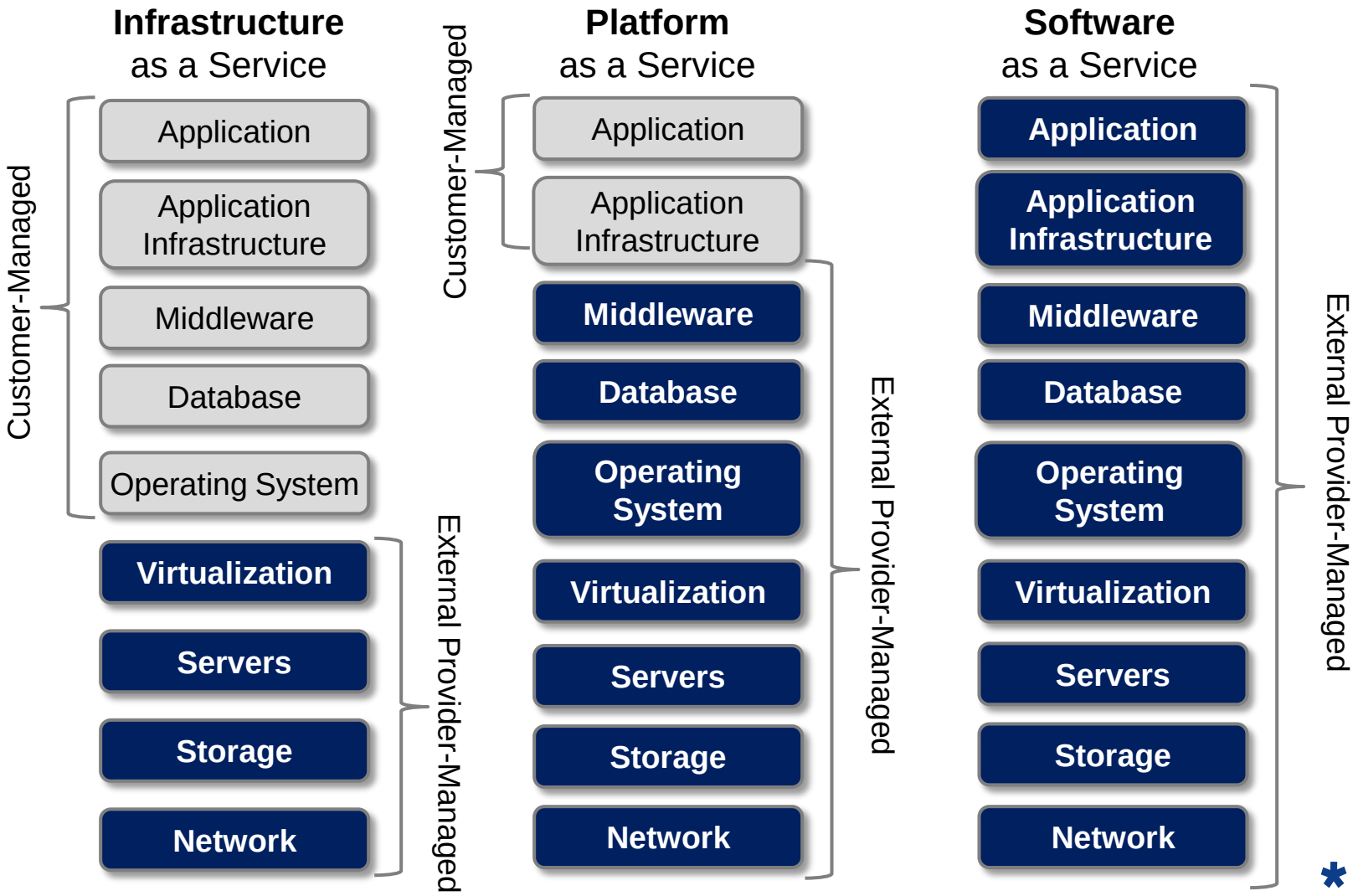
- Business Process as a Service
- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Deployment Models

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

ISG INFORMATION SERVICES GROUP

With a Clear Definition of the Service Delivery Models



ISG INFORMATION SERVICES GROUP

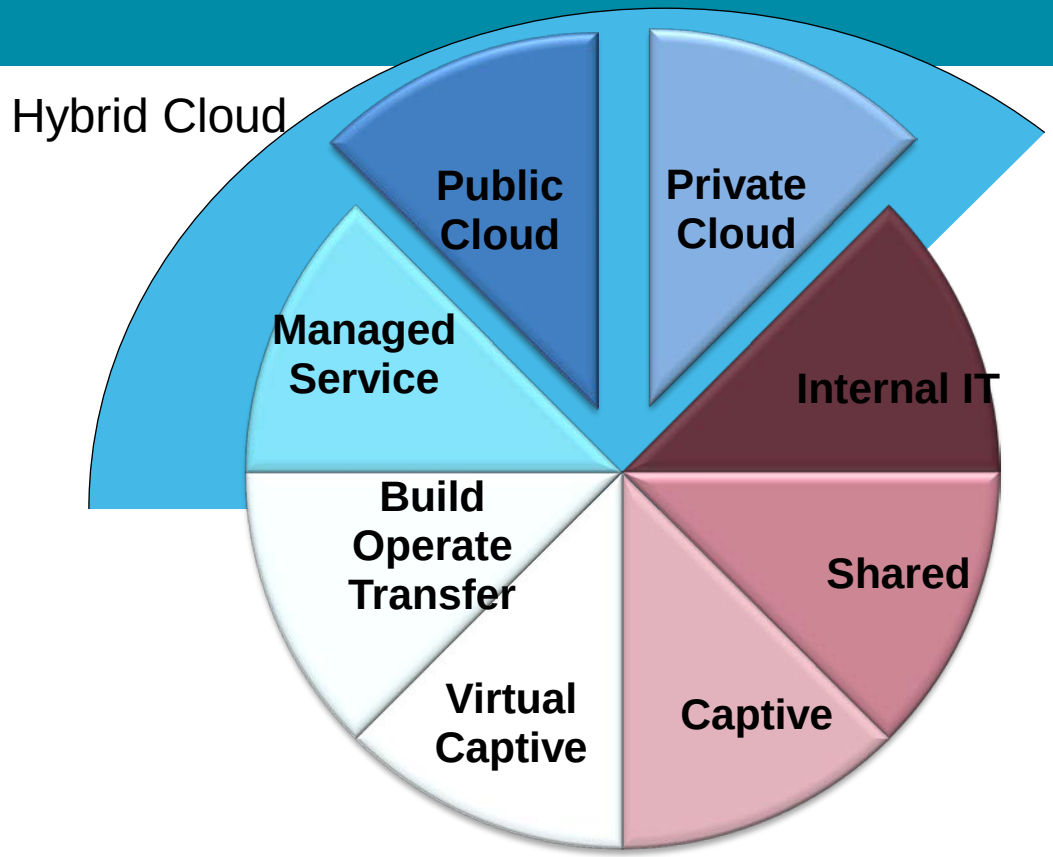
The Diversity of Cloud Solutions is Growing

- In the “cloudy” beginning there was the public cloud, e.g., Amazon & Google

- Then the marketplace added
  - Private clouds (dedicated cloud environment)
  - Hybrid clouds (managed hosting, private and public cloud)
  - Community Clouds

ISG INFORMATION SERVICES GROUP

Service Delivery Options



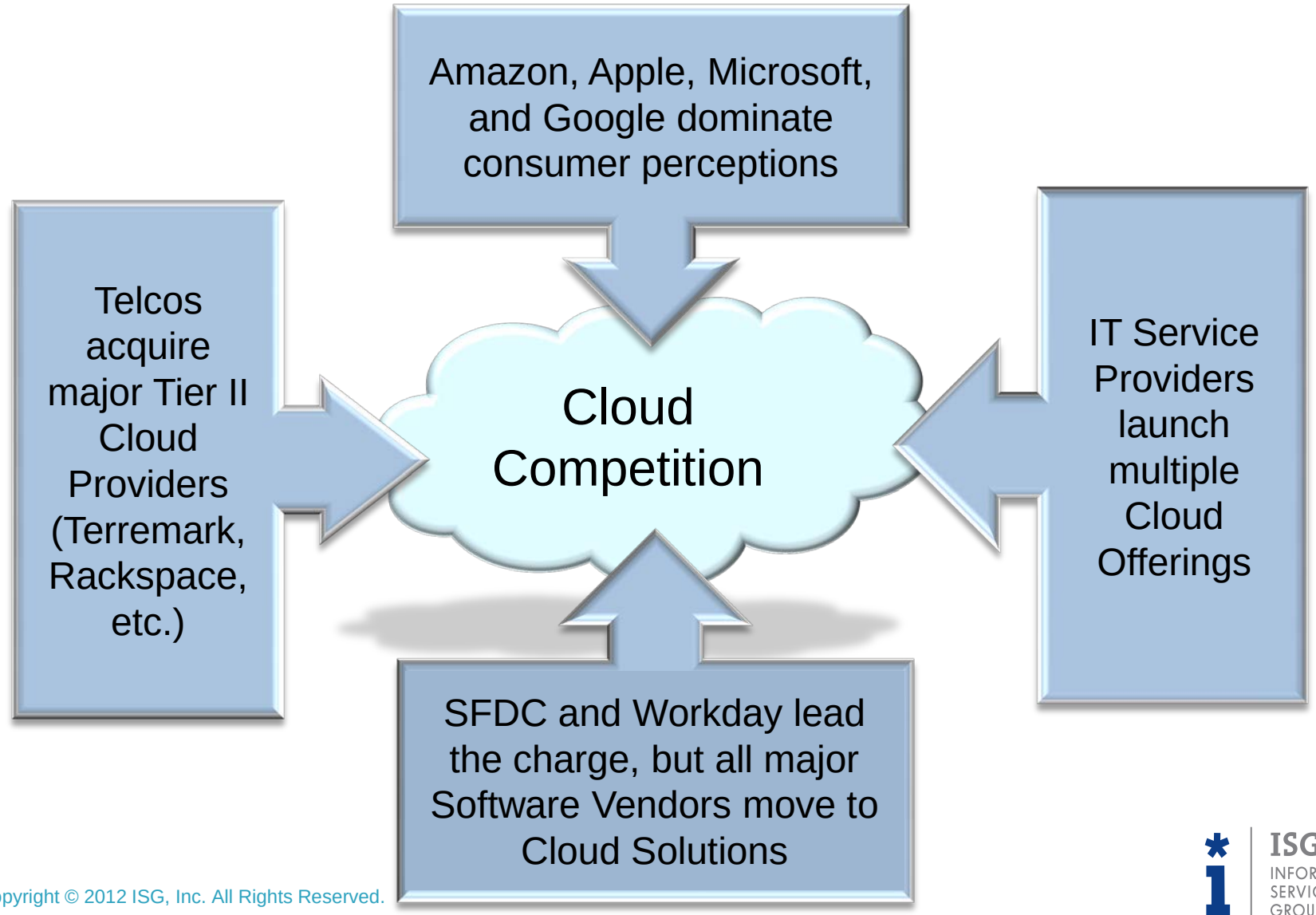
A variety of IT service delivery models are in place at most companies. Cloud services typically will have integration points with other service delivery models.

ISG INFORMATION SERVICES GROUP

Clouds Complicate the Corporate IT Strategy Agenda

ISG INFORMATION SERVICES GROUP

With Intense Competition Building in the Market



ISG INFORMATION SERVICES GROUP

Current Market Drivers

- Consumer experiences are pushing commercial markets toward Cloud Computing practices
- Niche players are providing compelling stories forcing traditional market leaders to follow suit
- Many benefits are being touted including speed to market, cost savings, flexibility, and minimized capital investment
- CIOs are being told the Cloud is the way to go and feel they are missing out

ISG
INFORMATION
SERVICES
GROUP

Data Security in the Cloud Is a Real Concern!

- Data Ownership and Portability
- Access to Data
- Data Borders (Geo and Privacy Laws)
- Data Co-mingling
- Discovery
- Security Breaches

ISG
INFORMATION
SERVICES
GROUP

Ownership and Access Are at the Top of the Risk List…

- Data Ownership and Portability
  - Do contract terms specify customer ownership and control?
  - Can the service provider ensure that client data can be purged from its cloud?
  - Can the data be retrieved efficiently and in a usable format?

- Access to Data (e.g., HIPAA, PII, PCI)
  - Who is permitted to access the data?
  - What government “flow down” provisions are required?

ISG INFORMATION SERVICES GROUP

Navigating security in the Cloud

Challenges

- Wider adoption of cloud services, e.g., by suppliers
- More diversity and complexity of cloud services

Marketplace “solutions”

- Standard cloud infrastructures, e.g., Vblock (Cisco, EMC, VMWare)
- Standards bodies and certifications

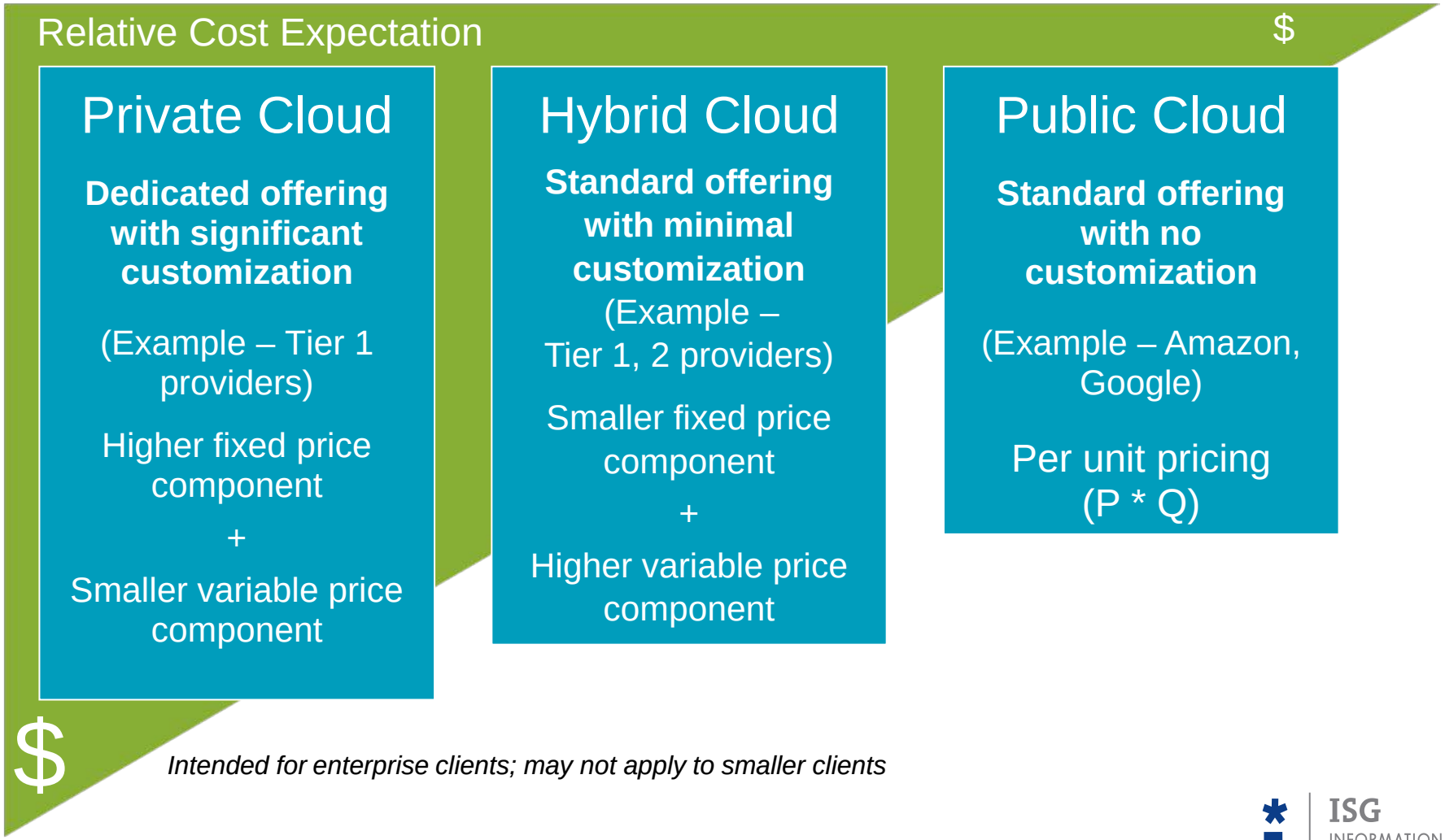
  Example: Cloud Security Alliance https://cloudsecurityalliance.org/

  – Security Guidance for Critical Areas of Focus in Cloud, v2.1

  – Certificate of Cloud Security Knowledge (CCSK)

ISG INFORMATION SERVICES GROUP

ISG's View on Current Pricing Approaches



Intended for enterprise clients; may not apply to smaller clients

ISG INFORMATION SERVICES GROUP

Cloud Pricing Observations

- There are many implications resulting from a shift to Cloud Computing - shifts are evolutionary, not revolutionary
- There are few pricing standards in Cloud Computing transactions -- observing some consistent practices and seeking to implement appropriate standards
- ISG has recommended pricing structures for each of the general types of Cloud transactions
- As has always been the case, it is impossible to separate the financial components of a transaction from the operational components; both sides must stay in sync

ISG
INFORMATION
SERVICES
GROUP

Commercial Impacts – Legacy Service Providers

- Transactions should include commercial terms and pricing considerations to enable migration to Cloud technology in the future
- Consider impacts to any minimum revenue commitment if a portion of the current agreement moves to a separate Cloud contract
- Include termination assistance language in the event some portion of the scope moves to Cloud
- Pricing structure should be flexible to allow committed and predictable cost for movement from legacy systems to Cloud systems

ISG INFORMATION SERVICES GROUP

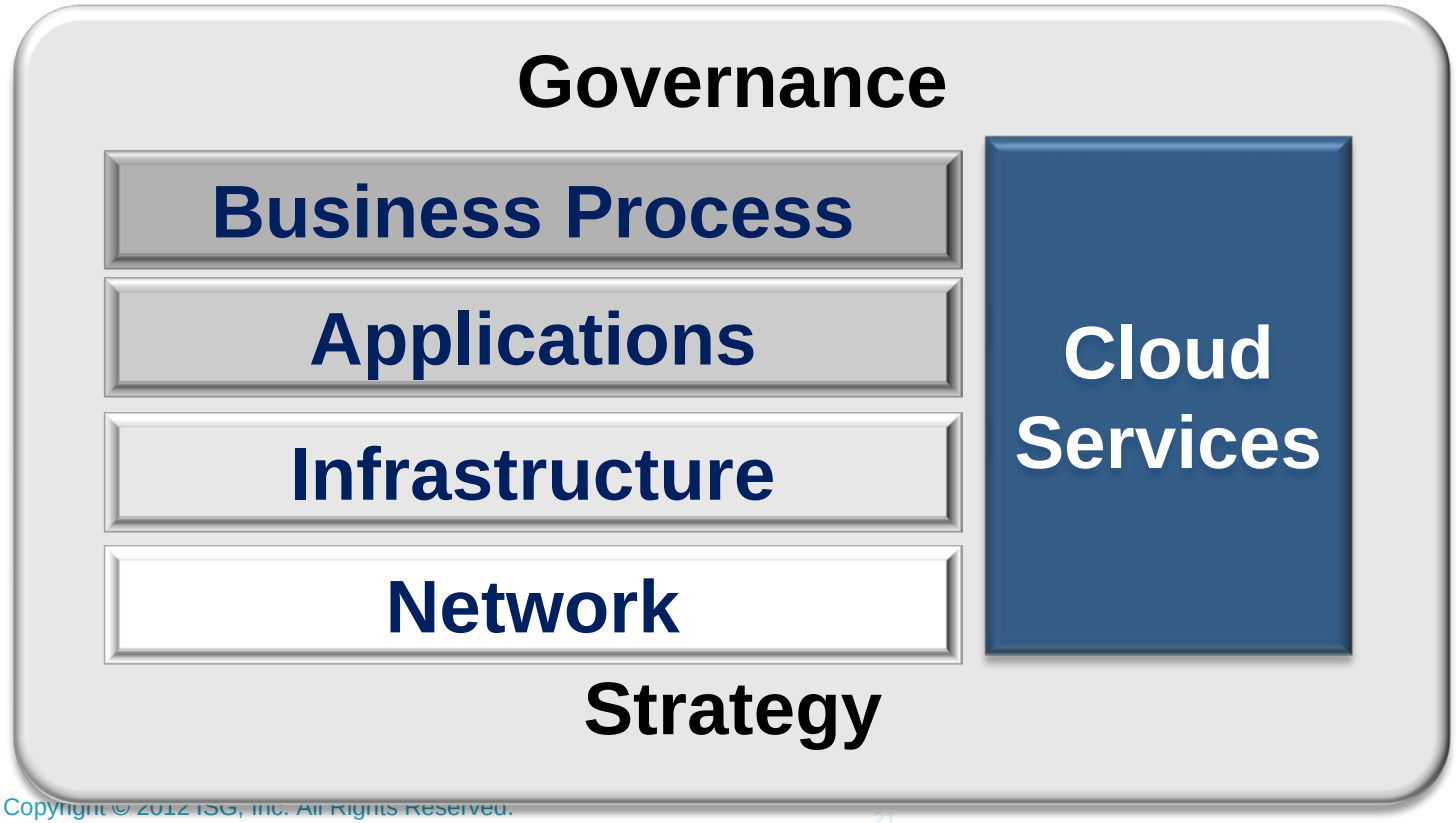
Commercial Impacts – Niche Providers

- Traditional MSA terms may not be acceptable, as they will have their own “standard positions” based on their consumer heritage
- Standard service level methodology may not be understood or acceptable
- May have less mature billing systems
- Year-over-year pricing improvements may not be committed as in a legacy transaction

ISG
INFORMATION
SERVICES
GROUP

Cloud and the Sourcing Lifecycle

- Cloud is more than technology – new operating models are evolving that penetrate all aspects of the sourcing lifecycle



ISG INFORMATION SERVICES GROUP

Managing Mobile Devices in the Workplace, Including a Look at Social Media Issues

Rapid, Exponential Growth – Mobile Service

- 1982
  - Cellular service approved in United States
- 1990
  - 1 Million mobile accounts in United States
- 2000
  - 12% of world population has a mobile account

Rapid, Exponential Growth – Mobile Service

- 2011
  - 5.7 billion mobile accounts (equivalent of 87% of world population)
  - 960 million mobile accounts in China
  - In United States and EU – more mobile accounts than people (1.2 accounts per person)

Rapid, Exponential Growth – Mobile Text

- 1993
  - First text message sent
- 1998
  - First Blackberry shipped
- 2011
  - 6 trillion text messages sent
  - 12 trillion email messages sent
  - 95 trillion spam email messages sent

Rapid, Exponential Growth – Mobile Web

- 2007
  - First iPhone shipped
- 2011
  - 490 million smartphones in use
    - *94 million – Samsung; 93 million – Apple; 77 million – Nokia; 51 million – BlackBerry*
  - Operating systems
    - *50% – Android (Google) (250% growth); 19% – iOS (Apple) (100% growth); 10% – BlackBerry (5% growth)*

Rapid, Exponential Growth – Mobile Tablets

- 2010
  - First iPad shipped
- 2011
  - 55 Million tablets sold (350% growth over 2010)
  - 80% of Fortune 100 companies deployed or developed mobile apps
  - 21% of purchased tablets for employees (51% to purchase tablets for employees in 2012)

Rapid, Exponential Growth – Not Just Text

- In 2011
  - Smartphone use:
    - *68% for news*
    - *50% conduct banking transactions*
  - Tablet users:
    - *Online time for work – increases 10%*
    - *Replacing PCs (PC growth – 10%)*
  - Mobile advertising:
    - *2010 – $1.6 Billion; 2011 – $3.3 billion; 2015 (est.) – $21 billion*

Rapid, Exponential Growth – Not Just Text

- Facebook
  - 2004
    - *Launched for Harvard*
  - 2006
    - *Launched to public*
  - 2008
    - *100 million users*
  - 2011
    - *800 million users worldwide (40% of U.S. residents)*

Outsourcing Impact – Mobile Service

- Cost of Service
  - Pricing
  - Pass Through Expenses
  - Third Party Agreements
- Global Footprint
  - Compatibility
  - Local Agreements

Outsourcing Impact – Mobile Service

- Quality of Service
  - Service Levels
  - Continuous Improvement/Benchmarking
- Technological Changes (Broadband)
  - Expertise
  - Term
  - Change Management

Outsourcing Impact – Mobile Text

- Security
  - Personal vs. Business Device
  - System Hacking
  - Lost Devices
  - Absence of Push Technology
- Legal Liability
  - Texting Bans

Outsourcing Impact – Mobile Text

- Document Retention
  - Align Policies
  - Ongoing Storage
  - Destruction Safeguards

Outsourcing Impact – Mobile Web

- Shared resources
  - Employee vs. Employer
  - Vendor vs. Customer
- Technology Issues
  - Compatibility
    - *Apple/Android*
  - App Development
    - *iTunes Issue*

Outsourcing Impact – Mobile Tablets

- Replacement of PCs
  - Equipment Purchase/Lease
  - Shared Resource
- Expertise
  - Compatibility
  - App Development
  - Network Security

Outsourcing Impact – Social Media

- Align Policies
  - Policy Development/Modifications
  - Supplier/Client Employees
- Customer communications
  - Ban vs. Embrace
- Document Retention
  - Facebook/Texting
- Confidentiality

Re-Evaluating Security Requirements in a Web-Based World

What We Want to Accomplish

- The Conundrum
- Security and the “Cloud”
- Security and Remote Workers of the Outsourcer
- Handling Cyber Data Breaches in the Contract
- Key Reminders

The Conundrum
In What Outsourcing Customers Want …

Leverage web-based technologies to create outsourced solutions that are:

smarter

faster

more elastic

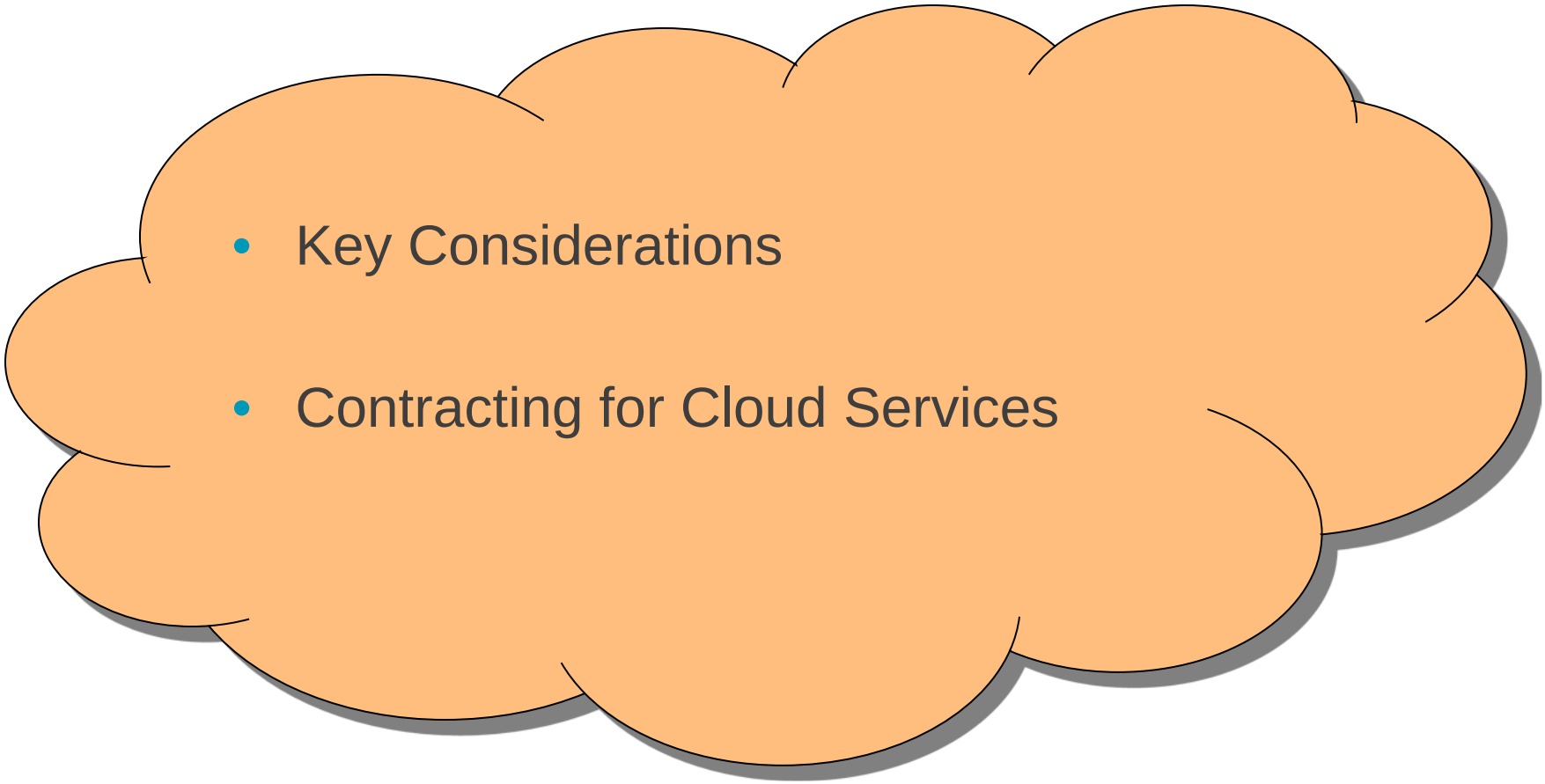
less expensive

And at the same time ***not compromise*** *security, control or content ownership*

Can You Have It All …

- It may depend upon:
  - ✓ Solution
    - *Private vs. public (or hybrid)*
    - *Standard vs. customized*
    - *Functional requirements*
    - *Security controls*
  - ✓ Appetite and readiness for change
  - ✓ Data being processed/accessed
  - ✓ Contract

Security and the Cloud



- Key Considerations
- Contracting for Cloud Services

Security and the Cloud – Key Considerations

Understand the what, where, who and how

- ✓ **What** is the security offering vs. **What** are the security requirements
- ✓ **What** types of data will be processed/hosted
  - – Personal information, PCI, business sensitive information
- ✓ **Where** are the services being provided
- ✓ **Who** is providing the services
- ✓ **How** is data segregated and used
  - – May vary by environment (production, DR, back up, archive)

Work with Security, Audit, Risk, DR, Compliance

Security and the Cloud – The Contract

- Security requirements
  - Compliance with internal vs. provider policies – can they be aligned? What is incorporated into the contract?
    - *Starting point*
    - *Bridging the gaps for signing and after*
    - *Hybrid security solution?*
  - Acceptable use policies
    - *What are they?*
    - *Surveillance rights*
    - *Beware of standardized/generic terms incorporated by reference*

Security and the Cloud – The Contract

- Handling change
  - **Balancing** control and benefits of a leveraged model
  - Right to change security requirements
    - *Transparency - Will you know?*
    - *Notice and/or approval*
  - Customer vs. provider required change
    - *Mandatory vs. discretionary*
    - *Can the systems be partitioned?*
  - Currency requirements
    - *Update requirements (good and bad)*
    - *Downtime*

Security and the Cloud – The Contract

- Examples of changes that can be made without approval
  - Changes that do not materially adversely impact the customer, the end users, the services
  - Changes that do not result in security risk, noncompliance with laws or additional costs to customer
  - Changes that are consistent with industry standard?
- Examples of when provider pays for change
  - Change to compliance with law?
  - Change made across multiple customers?
  - Change necessary to stay current?
  - Note: Customization may = $$

Security and the Cloud – The Contract

- Service locations
  - Need to know where your data is
  - Primary and back up
  - Right to change
- Personnel
  - Background checks??
  - Training; certifications
  - Right to subcontract

Security and the Cloud – The Contract

- Compliance
  - Internal requirements (not just security)
  - External Standards
    - *ISO*
    - *SSAE16*
    - *PCI*
      - Is provider certification enough; Customer controls still required (point to point encryption; tokenization)
    - *Cloud standards??*

Federal Risk and Authorization Management (FedRAMP)

sets standard approach to security assessment, authorization and continuous monitoring … baseline controls coming soon

STAR (Cloud Security's Alliance Security Trust and Assurance Registry)

public repository for provider security controls; members fill out a questionnaire

Security and the Cloud – The Contract

- Compliance
  - With laws, regulations and “guidance”
    - *US and beyond*
    - *Now and changes*
  - Privacy
  - Industry regulations (financial, insurance, pharma)
  - Import and export issues
    - *Focus on location of servers and personnel*

Security and the Cloud – The Contract
Focus on "Data"

Data segregation

- How is the data segregated?
- Check production and other environments
- Can you get it back (and at what cost?)
- Think about discovery implications

Data and software back up

- How and how often?
- Where and on what type of media?
- Regular delivery?

Access and audit

- Right to access data?
- Right to audit/perform reviews
- Quality/ compliance certifications
- Costs

Ownership and right to use

- Software
- Data and content
- Reports
- Performance data
- Data analytics

Security and the Cloud – The Contract

- Liability
  - Data breaches
  - Service outage
- Termination
  - When and by whom?
  - Right to suspend services?
- Unwinding the arrangement

Security and the Cloud – What It Means for the Contract

- Is it really different than what we have been doing in outsourcing deals?
  - Same issues
  - Shift in the paradigm
- Can the Customer create negotiating leverage?
- Finding a solution that works

Security and Remote Workers of the Outsourcer: Do you know where your resources are?

Security and Remote Workers of the Outsourcer

- Often no mention of remote access by workers of provider in the outsourcing contract
  - (IDC study) Estimates that worldwide mobile worker population will grow to 20% of workforce (1.19 billion people) by 2012
  - Aligning changing workplace with security needs

Security and Remote Workers of the Outsourcer

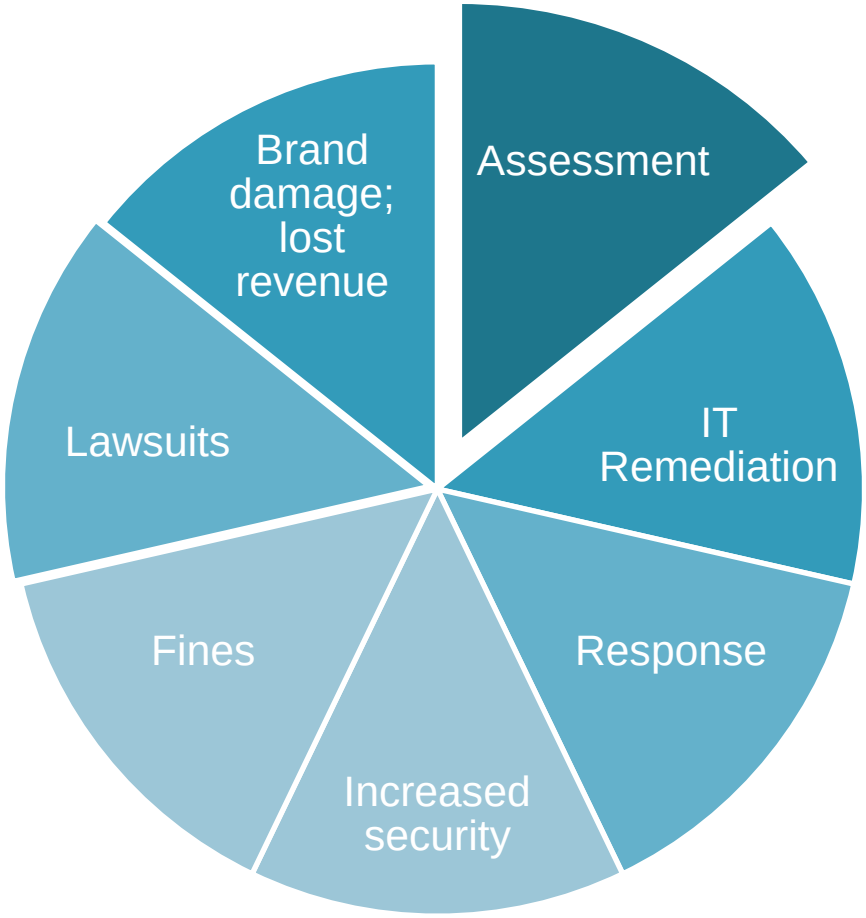
- Dealing with the reality in the solution
  - When is it ok?
    - *May be a cost issue*
      - Off hour coverage
    - *What type of data and system access*
    - *Tough to tie down managers*
  - What do your policies say? What should they say?
    - *Laptops, mobile devices, non-company devices, network connections*

Security and Remote Workers of the Outsourcer

- Dealing with the reality in the contract
  - Is your provider in breach?
  - Security requirements
    - *Examples: passwords, monitoring requirements, antivirus software, local storage, encryption, incident management*
  - Awareness and training

Cyber Data Breaches – and the Outsourcing Contract …

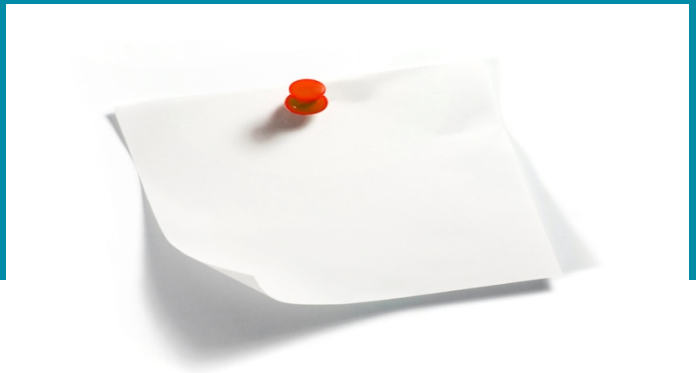
- When it happens …
  - Response and remediation
  - Allocation of responsibility
    - *Breach vs. non-breach*
    - *Should this be capped?*
- Cost of breach
  - (2011 Study by Ponemon Institute) Average time to resolve a cyber attack = 18 days; cost per data record = $214



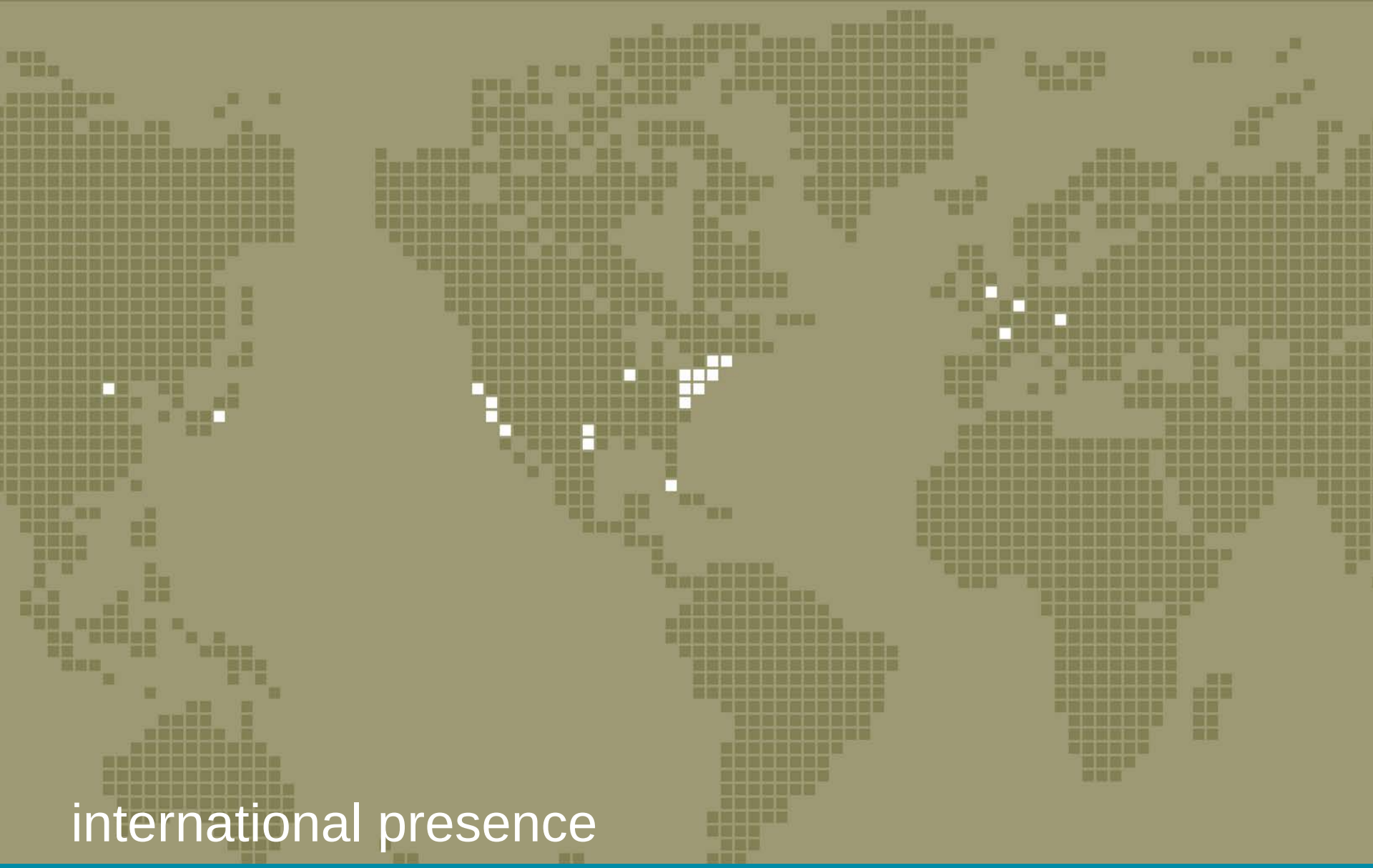
Cyber Data Breaches – and the Outsourcing Contract …

- Looking to Cyber Insurance
  - Customer and provider coverage
    - *Pre-conditions*
  - What is covered (Zurich American Insurance vs. Sony Corp of America)
    - *Limitations and amounts*
    - *Are acts of service providers covered under the privacy breach definition?*
    - *Good resources are available (e.g., checklist provided by Online Trust Alliance (OTA) in its 2012 Data Protection & Breach Readiness Guide)*

And A Few Key Reminders



- SEC Guidance
  - Assistance for assessing disclosures to be made re: cybersecurity matters/breaches (IT and finance to work together)
- Proposed Changes to EU Data Privacy
  - Standardized regulations (not directives) across member states
- Massachusetts Regulations – March 1, 2012 Trigger
  - Pre-March 2010 contracts may need to be amended
  - Not just for MA companies
- SSAE16
  - Updating the contract



international presence

Beijing Boston Brussels Chicago Dallas Frankfurt Harrisburg Houston Irvine
London Los Angeles Miami New York Palo Alto Paris Philadelphia Pittsburgh
Princeton San Francisco Tokyo Washington Wilmington