

IAOP Data Security Chapter Meeting Jan. 27, 2010



Theme:
**Security & Privacy
Regulations
Affecting Outsourcing
And How To Comply**

Co-hosted by JANUS Associates and Mayer Brown LLP
Held at offices of Mayer Brown, 1627 Broadway, New York City

MAYER • BROWN



Agenda

- Agenda and IAOP Overview Jim Adams – JANUS
- New Developments in Security & Privacy Laws Affecting Outsourcing Rebecca Eisner – Mayer Brown
- Practical Approaches to Compliance Karl Muenzinger - JANUS
- Panel Discussion Moderator: David Hudanish – Mayer Brown
Panelists: Phil Hausler – IBM
Benjamin Smith – BlackRock
John Mancini – Mayer Brown
Matthew Lane – JANUS

MAYER • BROWN



Changing Landscape in Privacy and Data Protection Impacts Outsourcing

IAOP Security Chapter Meeting – NYC Jan. 27, 2010

Rebecca Eisner

(312) 701-8577

Partner – Chicago, IL

reisner@mayerbrown.com

U.S. Privacy and Data Security Regulation

- Key Laws

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH)
- Fair Credit Reporting Act/FACT Act
- Federal Trade Commission Act (FTCA)
- ID Theft Red Flags
- State Security Laws (e.g., Breach Notification and Encryption)

U.S. Privacy and Data Security Regulation –

- Updates to HIPAA via HITECH and the American Reinvestment and Recovery Act (ARRA)
- Incorporates breach notification
- Increases individual rights to update information and prevent disclosure to affiliates
- Prohibition on the sale of PHI and restrictions on marketing of PHI
- Access to information and transfer of information must be tracked
- Connecticut Attorney General Blumenthal sues Health Net of Connecticut regarding the disappearance of a portable computer disk drive that Health Net confirms held protected health information and other personally identifiable data about 1.5 million current and former members

U.S. Privacy and Data Security Regulation

- FACT Act
 - Disposal Regulations
 - Financial institutions and other entities must develop and maintain controls to ensure that they properly dispose of certain “consumer information.”
 - “Consumer information” is “any record about an individual, whether in paper, electronic, or other form that is a consumer report or that is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the institution for a business purpose.”

U.S. Privacy and Data Security Regulation –

- FTCA
 - Section 5 of the FTCA prohibits unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45.
 - FTC has used Section 5 as the basis for some its recent enforcement actions in the privacy and data security area.
- The FTC intends to move forward with action to protect consumer online privacy -- FTC Chairman Jon Leibowitz, Dec. 7.
- FTC Chairman Jon Liebowitz said he favors consumer opt-in as a prerequisite to the use of personal information.
- FTC public roundtable on consumer privacy, Jan. 28, will cover the “privacy implications of several evolving technologies, including social networking and other platform services, cloud computing, and mobile computing”

U.S. Privacy and Data Security Regulation –

Banking/FTC ID Theft Red Flags Rule

- Entities issuing credit (including telecom, utilities, student loan providers) now have to monitor accounts for activity which may indicate identity theft.
- Compliance required in 2009
- 26 examples of potential red flags in guidance in five key areas:
 - Alerts, Notifications or Warnings from a Consumer Reporting Agency
 - Suspicious Documents or Personal Identifying Information
 - Unusual Use of, or Suspicious Activity Related to, the Covered Account
 - Notice Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Creditor

U.S. Privacy and Data Security Regulation –

- State Data Security and Breach Laws
 - Absence of comprehensive federal legislation has prompted state legislation – federal legislation proposed.
 - 45 states, Washington DC, Puerto Rico and the Virgin Islands have breach notification and/or data security laws that protect their citizens.
 - Most state laws define sensitive data as including an individual's last name and first name (or first initial) combined with a Social Security number, driver's license or identification card number, or financial account number plus password or access code.
 - There are exceptions (California, most notably).

U.S. Privacy and Data Security Regulation –

- Nevada Laws
 - Require encryption of (1) electronically transmitted data and (2) data stored on portable devices transported off-site
 - Data collectors collecting payment card data must comply with PCI DSS.
- Massachusetts Data Security Regulations
 - Beginning March, 2010, these regulations require a comprehensive security program and encryption of transmitted data
 - Apply to any party, in any state, that owns, licenses, stores or maintains the personal information of a Massachusetts resident
- New York: issued a comprehensive privacy guide
- California: health care privacy laws

Litigation & Enforcement Actions (examples)

- *Certegy Check Services v. Lockwood*
- *Pisciotta v. Old Nat'l Bancorp*
- *In re TJX Cos. Retail Security Breach Litig.*
- *In re Hannaford Bros. Co. Customer Data Security Breach Litig. (multi-district)*

Litigation & Enforcement Actions

- FTC Enforcement Actions
 - Violations of GLBA safeguarding or privacy rules
 - Unfair or deceptive acts or practices
 - Violation of the disposal rule
- FTC has filed at least 23 cases challenging data security practices:
 - CVS Caremark (Feb. 18, 2009) (unsecured trash)
 - Genica Corp (Feb. 5, 2009) (hacker)
 - Premier Capital Lending (Nov. 6, 2008) (hacker)
 - TJMaxx (Mar. 27, 2008) (hacker)
 - Reed Elsevier and Seisint (Mar. 27, 2008) (inadequate security)
 - ValueClick (Mar. 17, 2008) (SQL injection)
 - Goal Financial (Mar. 4, 2008) (employee conduct)
 - Online Apparel (Jan. 17, 2008) (SQL injection)

Litigation & Enforcement Actions

- State Actions

- 41 states vs. TJX Cos. (TJ Maxx's parent): \$9 million settlement
- *Texas v. CVS Pharmacy, Inc.*, Tex. Dist. Ct., No. CV-72881 (settlement entered Mar. 25, 2008)(paid state \$315,000 for allegedly tossing personal information into the garbage without shredding)
- Ky. Att'y Gen. conducts sweep to investigate compliance with consumer record disposal law (Nov. 2007) (Office of Consumer Protection notifies 33 businesses of their violations)
- *Hawaii v. Marn*, Haw. Cir. Ct., No. 07-1-0524-03 EEH, (settled July 19, 2007)(escrow company paid \$10,000 fine for allegedly failing to properly dispose of sensitive customer information)

EU Data Protection and Data Transfers

- EU Directive and Swiss Data Protection Act prohibits the disclosure of EU/CH personal data to third countries who do not provide an adequate level of data protection unless one of very limited options, subject to local data privacy legislation, applies.
 - Switzerland, Argentina, Canada, Isle of Man, Guernsey, Jersey, Israel and Andorra are considered adequate by the EU. (EU is also considered adequate by Switzerland).
 - US companies that certify to the EU-US Safe Harbor Framework are considered “adequate” by the EU.
 - US companies that certify to the Swiss-US Safe Harbor Framework are considered “adequate” by the Swiss Data Protection Authority.

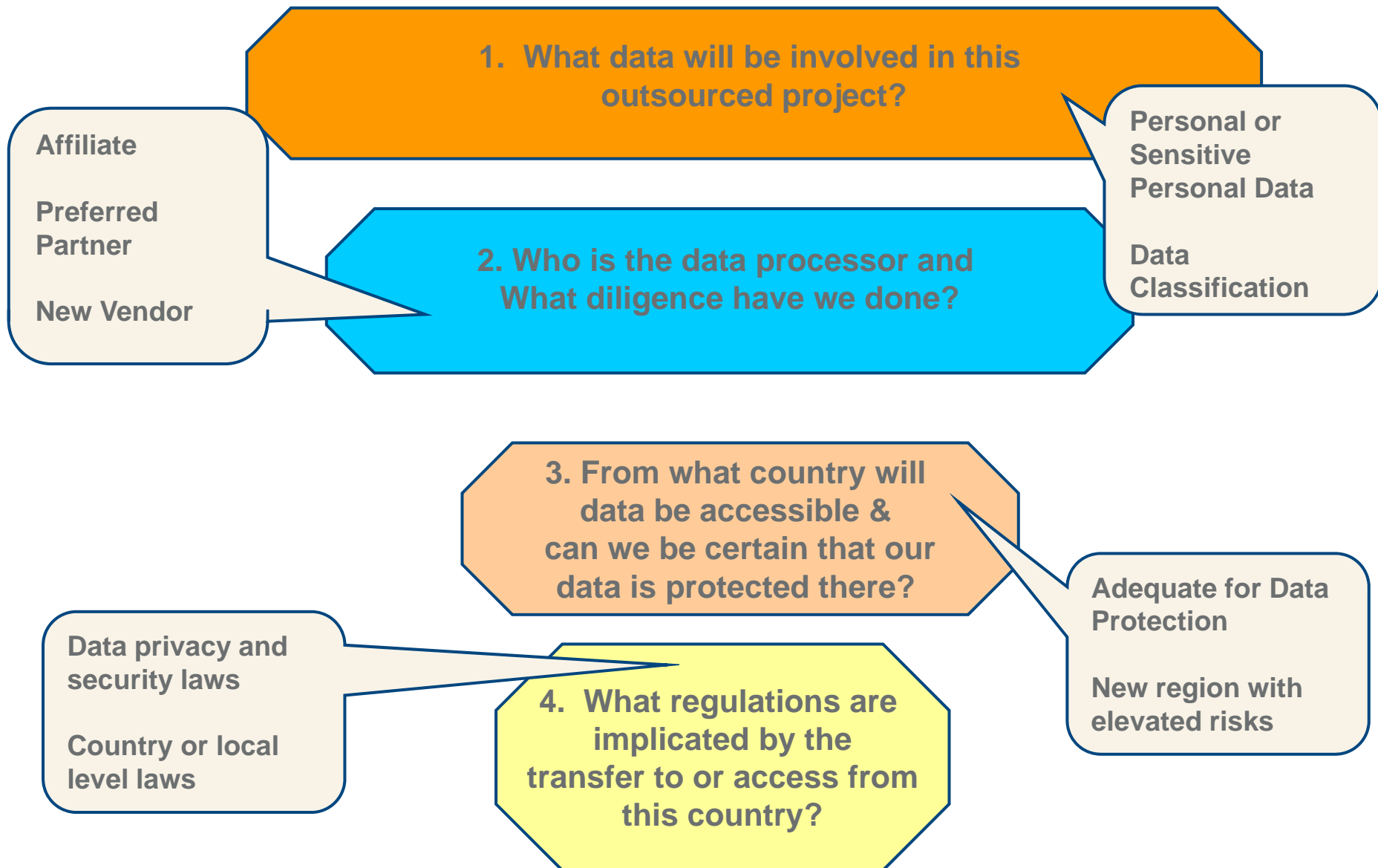
European Data Protection and Transfer

- Multi-nationals who undertake global projects where data will be centralized must consider personal data protection issues
- These include both transfers among affiliates of data (e.g., all data flowing to US data center for ERP project), AND transfers to third parties
- “Transfer” does not mean file transfer or moving a server – it can mean ability to view data from a location outside of the jurisdiction

Risk Management in Outsourcing

- Customers cannot deflect responsibility or liability for privacy and security compliance by outsourcing to a provider
- Beyond vague “reasonable security” standards, or technical solutions, the legal standard for privacy compliance is emerging as a process:
 - access assets and risks, plan, implement, monitor, report, repeat and evolve
 - ensuring compliance with third party providers is key to this process – including due diligence
- The contract is only one part of risk management

Risk Management: Key Questions



Key Contract Terms: Customer Must Have Topics

- Specific Privacy Requirements for Personal Information (including processing and transfer locations)
- Security Requirements
- Change Control
- Reporting Requirements
- Audit Requirements
- Subcontracting Approval Rights and Flow Down of Provisions
- Incident Plans
- Breach notification
- Changes in Requirements
- Liability
- Costs

Trends for 2010 and Beyond --

- Business is becoming more global as regulation increases –especially in privacy and security
- Increased regulation will drive service offerings to address key regulatory challenges
- Regulatory requirements are impacting deal structures:
 - Global data project – business process designs to meet privacy and security regulation
 - Global email system – system design must take into account data transfer and data privacy requirements, as well as other regulatory requirements
 - Global spin off of unit – what happens when co-mingled data suddenly has two different owners around the globe?
- Allocation of risk and responsibility for privacy and security compliance will take center stage in contract negotiations

Clouds on the Horizon?

- Cloud Computing offers great opportunities and challenges
- Microsoft GC has called for the “Cloud Computing Advancement Act” that will promote innovation and protect consumers
- Many consumers and individuals use cloud computing applications already
- Study commissioned by Microsoft:
 - 84% of Americans use web mail service
 - 57% store or share information using a social media site
 - 33% store photos online
- The privacy, security and international issues with cloud computing are far from settled

Questions?

JANUS Associates

Compliance Strategy: A Practical Approach to Vendor Assessment

The International Association of Outsourcing Professionals (IAOP), Security Chapter

Karl W. Muenzinger, CISA CISM CISSP MBCI

January 27, 2010



Topics

- Vendor Security Compliance Affects Every Industry
- Managing the Scope of Vendor Assessments
- Managing the Process of Vendor Assessments

Vendor compliance affects every industry

Customers are required to monitor the security of their vendors

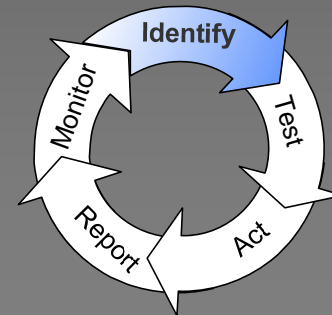
Vendor compliance requirements by industry

Financial Services	FFIEC GLBA SOX FDIC FACTA BASEL II PCI DSS	Federal Financial Institutions Examination Council : IT Examination Handbook <ul style="list-style-type: none"> • Supervision of Technology Service Providers (2003) • Outsourcing Technology Services (2004) Gramm-Leach Bliley Act of 1999 Sarbanes-Oxley Act of 2002 IT - Risk Management Program, IT Officer's Questionnaire of 2007 Fair and Accurate Credit Transactions Act Disposal Rule Sound Practices for the Management and Supervision of Operational Risk Payment Card Industry Data Security Standard
Healthcare	HIPAA ARRA HITECH	Health Insurance Portability and Accountability Act of 1996 American Recovery & Reinvestment Act Health Information Technology for Economic & Clinical Health Act of 2009
Government Services	FISMA ---	Federal Information Security Management Act of 2002 State and Municipal Statutes
All Sectors	FTC ---	Federal Trade Commission Act State Data Breach and Privacy regulations

Three Rules of Vendor Security Compliance

- Risk cannot be outsourced
- Compliance is Not Security, Security is Not Compliance
- Risk Management is the New Compliance Target

Risk Management :
An ongoing cycle of continuous improvement



Vendor Assessment Project Management : Finding the Balance between Time and Scope

Example of vendor assessment effort

400	Policy and Procedure questions (20 questions, 20 Policies and Procedures)
600	Technical Questions (30 per technology, 20 technologies)
100	Governance Questions
1,100	Subtotal: Questions per assessment
X 30	Assessments
33,000	Total Number of Questions!

- Customer's point of view
 - thousands of answers to review! And that's not including the follow-up inspections!
- Vendor's point of view
 - Reluctance to share business-confidential or proprietary information
 - Disruption from the never-ending audit: "each customer sends us a different list of questions!"

Anticipate Scope

by proactively adopting a common compliance framework :
COBIT, ISO 27001/27002, or NIST 800-53

Example : Scope of a HIPAA Audit		Common or Unique
Administrative Safeguards	Security Program , Roles and Responsibility Workforce Security Access Management Security Awareness and Training Security Incident Response Business Continuity and Disaster Recovery Risk Evaluation Business Associate Contracts	Common Common Common Mostly Common Common Common Common Somewhat unique
Physical Safeguards	Facility Access Controls Workstation Security Device and Media Controls	Common Common Common
Technical Safeguards	Access Control Audit Controls Integrity Authentication Transmission Security	Common Common Common Common Common
Organizational Requirements	Group Health Plans Policies, Procedures, and Documentation	Unique Mostly Common

Simplify Scope

Identify overlaps between Compliance Requirements

- Avoid separate compliance efforts for each regulation
- Align Policies and Procedures with common security controls

Common Security Controls	HIPAA	PCI	FFIEC	FISMA
Minimum Necessary Access to Confidential Information	X	X	X	X
Encryption of Confidential Data	X	X	X	X
User Awareness Training	X	X	X	X
Regular Penetration Tests and Vulnerability Assessments	X	X	X	X
Business Continuity and Disaster Recovery Plans	X	X	X	X
Physical Security	X	X	X	X
Change Management and Procurement Practices	X	X	X	X
..... More				

Reduce Scope

by segregating your customer systems and data

- **PCI:** Segregate your network, for a potentially huge cost savings
- **GLBA/FFIEC:** Separate financial customer data from internal support and administrative systems
- **HIPAA:** Segregate Health Records and processes to reduce HIPAA requirements for the rest of the organization



Risk Based Vendor Assessment

- **Identify** Vendors
- **Prioritize** by Risk
- **Assess** Using a Tiered Approach
- **Record** Proof of the Assessment Process
- **Repeat** Annually, and on Contract Renewal

Sample of a Tiered Assessment	Low	Medium	High
1) Business Agreements	X	X	X
2) Questionnaires and check lists	X	X	X
3) Review of Policies, procedures, and documentation		X	X
4) Independent Vulnerability Assessment and Penetration Test		X	X
5) Interviews		Optional	X
6) Standardized Reports:	Optional	Optional	X
SAS 70 Type II, BITS/Shared Assessments, HITRUST, ISO 27002 certification			

Questionnaire Design:

Ask Once, Comply Many Times

Vendor Assessment Question	Answer	HIPAA	PCI DSS	FFIEC
Do you keep an Inventory of your Confidential data	Yes	X	X	X
Is Confidential Data Encrypted during Transmission	Yes	X	X	X
Is Confidential Data Encrypted when stored on Disk or Tape	Yes	X	X	X
Independent Vulnerability Assessment in the last 12 months?	Yes	X	X	X
Have Contingency Plans been tested in the last 12 months?	Yes	X	X	X
..... More				

Governance, Risk Management and Compliance (GRC) Tools :

Common Features

- Crosswalk of Compliance Requirements
- Web-based Vendor Compliance Questionnaires
- Questions are mapped to crosswalk of compliance requirements
- Central Database of Answers and Supporting Documents
- Central tracking of Compliance Gaps
- Workflow for Remediation, Risk Management

Strategies for Customers To Simplify the Assessment Process

- Require the vendor to supply third party reports
 - Vulnerability Assessments conducted by independent experts, SAS 70 Type II, BITS/Shared Assessments, HITRUST, ISO 27002 certification
- Automate the collection of compliance data
 - using a Governance, Risk Management, and Compliance Tool (GRC)
- Outsource the vendor assessment process

Strategies for Vendors

To Simplify the Assessment Process

- Align your security program with common security frameworks (ISO 27002, COBIT, NIST 800-53)
 - so that your security program maps to the questions asked during audits
- Maintain a Database of compliance questions and answers
 - using a Governance, Risk Management, and Compliance Tool (GRC)
- Provide standardized third party reports

The Regulators' Perspective on SAS 70 and other Standardized Assessment Reports

- Good starting point, but may not address the unique operational risks of the customer
- Point in time audits are not a replacement for an ongoing risk management process
- SAS 70 state the controls that the vendor has in place, but provides limited opinion on what might be missing
 - SAS70 Type I is not adequate : SAS70 Type II is preferred (and more expensive)

The FFIEC Perspective on SAS 70 and other Standardized Assessment Reports

“In **lower risk relationships** the institution may prescribe the use of standardized reports, such as trust services reports or a Statement of Auditing Standards 70 (SAS 70) report.

However, “Financial institutions should evaluate carefully and critically whether a SAS 70 report adequately supports their oversight responsibilities.

The report may not provide a thorough test of security controls and security monitoring or address whether the vendor is meeting the institution’s specific risk mitigation requirements. “

Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook: Information Security, July 2006

Final Words

HONESTY BUILDS TRUST : TRUST LEADS TO INVESTMENT

- Total security is not achievable
- How a company approaches risk management is more important than the existence of risk
- Information security is an opportunity to build trust and bolster the reputation of your brand

Questions?



Panel Discussion:

"Managing the Security and Privacy Risks and Opportunities in Outsourcing"

Participants

Moderator: David Hudanish – Partner, Mayer Brown

Panelists: Phil Hausler – Vice Pres., Banking Industry, IBM

Benjamin Smith – Chief Info. Security Officer, BlackRock

John Mancini – Partner, Mayer Brown

Matthew Lane – Chief Technology Officer, JANUS

MAYER • BROWN



Thank You For Your Participation

Your Co-Hosts

JANUS Associates

Jim Adams

1050 Washington Blvd.
Stamford, CT 06901
Ph. 203-251-0238

Jima@JANUSassociates.com
www.JANUSassociates.com

Mayer Brown LLP

Rebecca Eisner

71 S. Wacker Drive
Chicago, IL 60606
Ph. 312.701.8577

Reisner@MayerBrown.com
www.MayerBrown.com



MAYER • BROWN

