I'M SECURE! WHO NEEDS A PRIVACY PROGRAM?

George G. McBride
I/T Shared Services
Johnson & Johnson Services, Inc.

Session ID: GRC-304
Session Classification: Intermediate

AGENDA

- Introduction and Challenges
- Privacy Program
- Program Execution
- Next Steps

Introduction and Challenges

What is Privacy and Why does it matter?

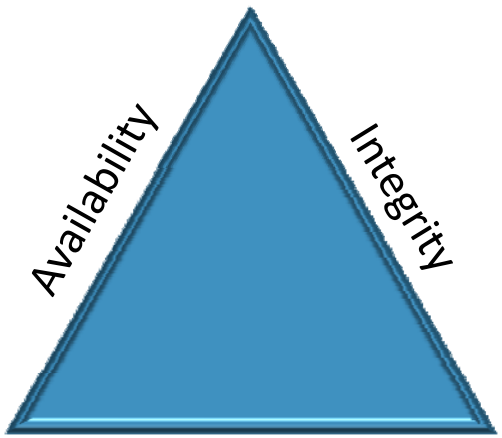
PRIVACY INTRODUCTION

Privacy - The rights and obligations of individuals and entities with respect to the processing / management of their information. Typically PII or PHI.

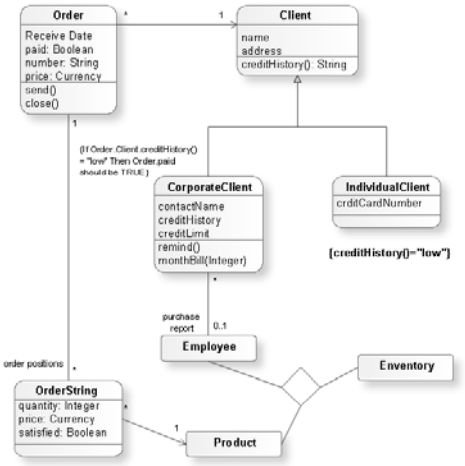
Management activities include: collecting, receiving, holding, examining, altering, processing, transferring, archiving, and destroying.

- Personally Identifiable Information (PII)
  - Information that can be used to uniquely identify, contact, or locate a specific individual
- Personal Health Information (PHI)
  - Information about health status, provision of health care, or payment for health care that can be linked to a specific individual

SECURITY & PRIVACY RELATIONSHIP



+



=

Security

Confidentiality: Access to data is limited to authorized resources

Integrity: Assurance that the data is authentic and complete; changes to the data are restricted to authorized entities

Availability: Data should be accessible, as needed, by those who are authorized

+

Usage: Appropriate use or management of the data

=

Privacy

You can have security without privacy, but you cannot have privacy without security.

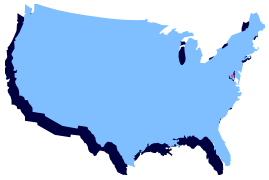
THE ROAD IS FILLED WITH CHALLENGES

- Where does Privacy fit within the Enterprise?
  - Within the Organization?
- What are your legal and regulatory requirements?
- Do you have Legal / General Counsel support?
  - If not, how can you get it?
- How do you work with the Information Security group?
- What is the budget and resource allocation?
- What is the scope of the program?
- Who is doing anything “Privacy” related today?
- Are there immediate requirements or expectations?

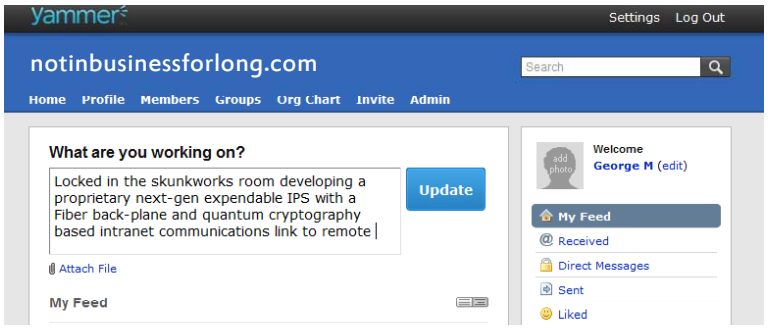
Have these questions answered before proceeding. It makes the job a little bit easier.

DOES IT AFFECT YOU?

- States With Privacy Regulations
- Alphabet Soup:
  - COPPA, FCRA, FERPA, GLBA, HIPAA , HITECH
- US Federal Privacy Regulation Legislation
- Countries From Argentina to Vietnam
- Extremely varying amounts of information, interpretation, case-law, enforcement and penalties
- It's A Global Economy:
  - business partners, customers, and employees can be located anywhere.
  - Businesses depend on global transfers of data



THINK PRIVACY DOESN'T AFFECT YOU? THINK WEB 2.0



Privacy Program

Defining and building the program

THE FOUNDATION

Scope	• Defines the overall scope of the program • Business unit, organizational, or enterprise wide • Geographic boundaries and local laws will influence decisions • Centralized versus de-centralized

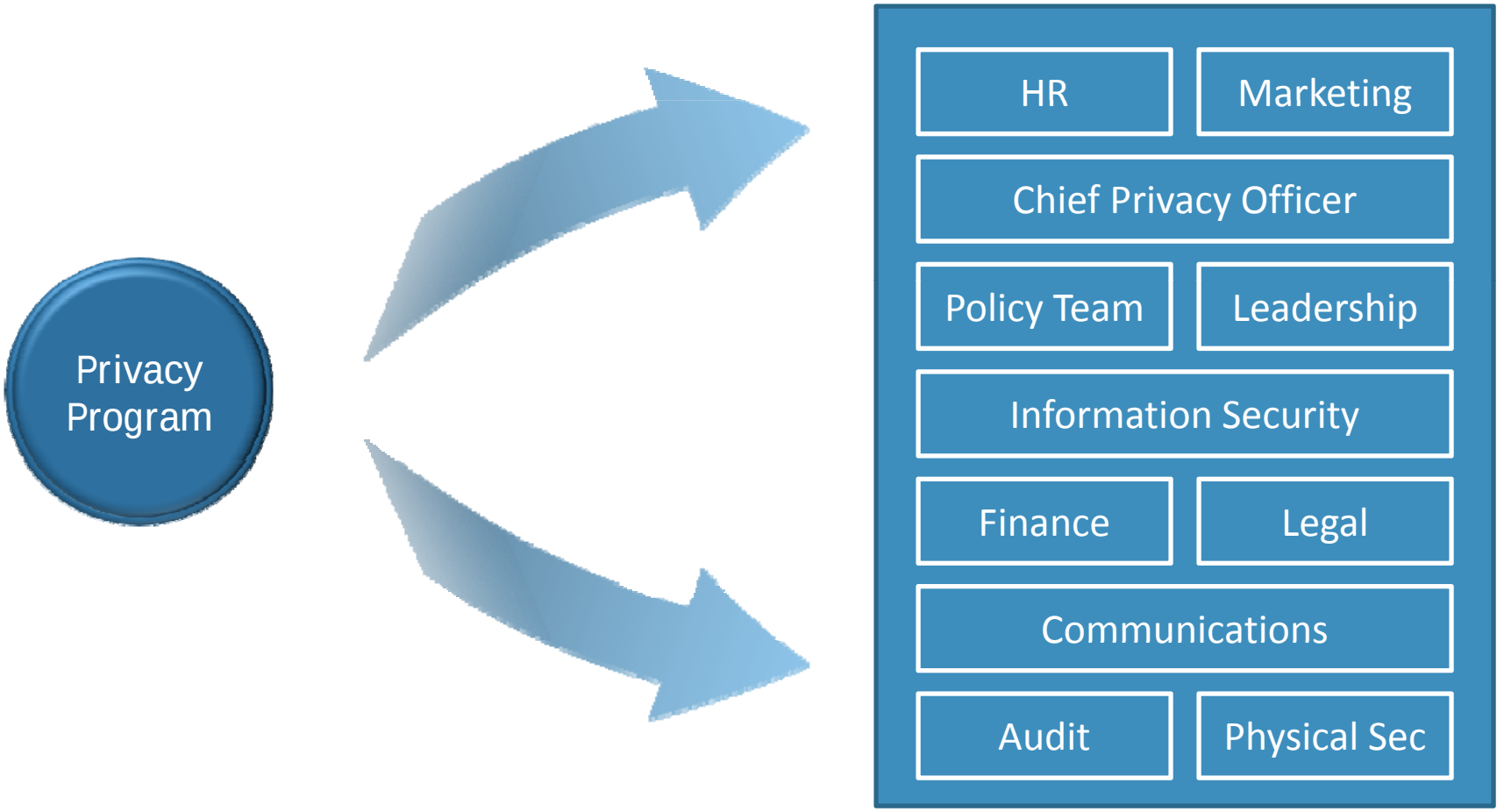
Mission	• Provides the rationale of why the Privacy Program exists:
	  • Manage the appropriate use of PHI and PII
	  • To “Reduce Privacy Risk” and “Protect Customer Data”
	  • Avoid fines and keep the company Officers out of jail

Governance	• Defines who oversees the Privacy Program • Defines the Privacy reporting structure and Accountability • Defines the responsibilities of the Privacy Program • Mechanism to drive change and advance the Privacy Program

These define the Privacy Program and resolve many Security versus Privacy conflicts.

THE FOUNDATION: PRIVACY FUNCTIONS

PRIVACY PROGRAM: IT'S ALL ABOUT WHO YOU KNOW

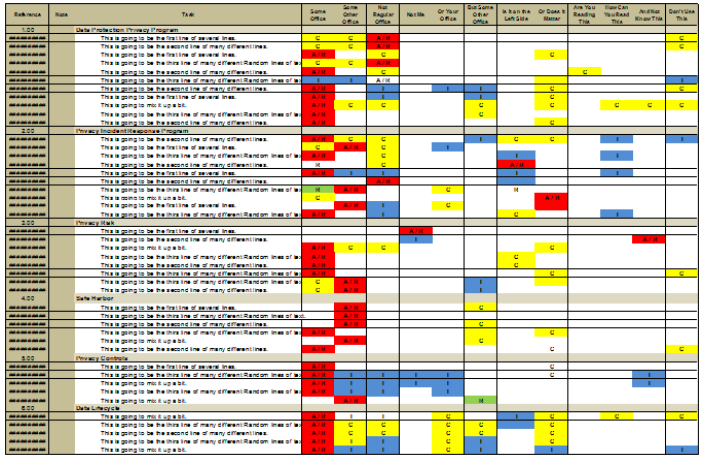


AND HOW YOU TELL THEM…

- Identify those organizations, people, and roles that you'll be interfacing with:
  - Internal and External
- Communications that are short and frequent
- Utilize existing communications mechanisms
- Carefully choose new communications mechanisms:
  - Privacy Council Meetings
  - Privacy Alerts
  - Incident Response Communications
    - And perhaps other "exceptions" to the normal communications channel
- Estimate frequency and resource needs
  - What do they need to do with what you tell them?

WHO DOES WHAT: ROLES AND RESPONSIBILITIES

- Once “what” has to be done has been defined:
  - Now you have to define “who” will do it
- Support may come from:
  - IT
  - Other Privacy Functions
  - Compliance / Regulatory Office
  - Information Security
  - Training and Awareness
  - Policy Development Team
  - Employee Hotline and Reporting Teams
  - Communications
  - Audit Teams
  - Customer / Business Unit Facing Teams



This is a critical step that requires input and discussions from all affected parties…

PRIVACY INCIDENT RESPONSE PLAN

- Needs to interface with and be compatible with the Security Incident Response Plan.
  - You do have one of those, right?
- Templates exist. The AICPA has developed a solid framework that can be tailored to your organization.
- Needs input, support, and approval from all parties.
- Legal's role includes how to react to PII/PHI breaches:
  - Notification to data owners, regulatory agencies, others
  - Timelines to make those notifications
  - Approvals of notifications, communications, actions
- Must be tested. Criticized. Commented on. Improved.

Arguably, the most important component of any Privacy Program.

PRIVACY TRAINING AND AWARENESS

Initial "All Hands" Training	• Delivered as quickly as possible
	• Establishes the Privacy Program
	• Gets the message out:
	  • (Re-) Introduces the Privacy Program
	  • Incident Response Program
	  • Roles and Responsibilities
	  • Where to go for additional resources
	• Information Classification deployment

Role Based Training	• Delivered after "All Hands" training
	• Provides detailed training:
	  • Privacy Officers
	  • Information Security Team
	  • Architects, Database Administrators, etc.
	• May be regionalized depending on local laws
	• Discussion of relevant controls and Privacy
	• May serve as an "All Hands" refresher course

The first opportunity to reach out to all employees. Make a great first impression!

DATA CLASSIFICATION

- Provides guidance to data-owners to classify and map their data into some number of categories:

Public	No PII	Public Information
Confidential	PII-A	Business Contact Info, Business Partner Information
Proprietary	PII-B	Personal/Emergency Contact Info, DOB, CRM Details
Restricted	PII-C	Bank Account Info, SSN, Medical History, Biometrics

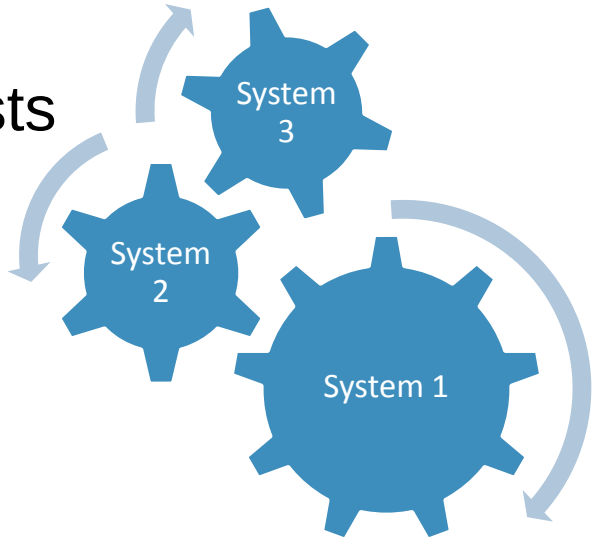
- May group various types of PII/PHI into those categories
- Provide training around the PII/PHI classification
- Provide tools and templates to assist the classification
- Responsibility of the data owner to classify the data

Program Execution

Reducing the Privacy Risk

DATA INVENTORY AND DATA FLOW

- Develop a methodology to capture the data and maintain the accuracy and currency of the data
- Listing of your “data” and where it exists
  - Data Owner and Custodian
  - Classification of Data
  - Last Update Date
  - Data Flow Sequence



- Generate Data Flows
  - Where it comes in / created through to where it leaves / archived
- Supports Incident Response Activities and Privacy Impact Assessments

An important task that will challenge your ability to enlist the support of others.

PRIVACY IMPACT ASSESSMENTS: MEASURING RISK

- Methodology to conduct Privacy Impact Assessments
- Identify the assets to review
  - After Inventory, Classification, and Controls Catalog completed
- Develop a prioritized risk approach
  - Controls Deployment
  - Areas of Focus
- Who will execute the Assessment?
  - Asset Owner
  - Privacy Officer
- Track Remediation
- Improve Process
  - Feedback

$$\text{Risk} = \frac{\text{Threat*} \times \text{Vulnerability}}{\text{Control}}$$

**Includes Likelihood And Impact Factors*

METRICS

- Start collecting data:
  - Management will ask for data. You'll want to see them as well.
- SMART
  - Specific. Measurable. Actionable. Relevant. Timely.

Sample Metrics	
Training	• Associates passing Training quiz on first try • Incident Reporting Hotline Calls
Lost Laptops	• Lost laptops investigated • Roll-out of Hard Drive Encryption
Privacy Impact Assessments	• Privacy Impact Assessment Completed • Percentage with Significant Findings • Internal/External web-sites reviewed
Data Inventory	• Data Assets Identified • Percentage of Data Assets with details captured

Next Steps

Keeping it going. Today and tomorrow.

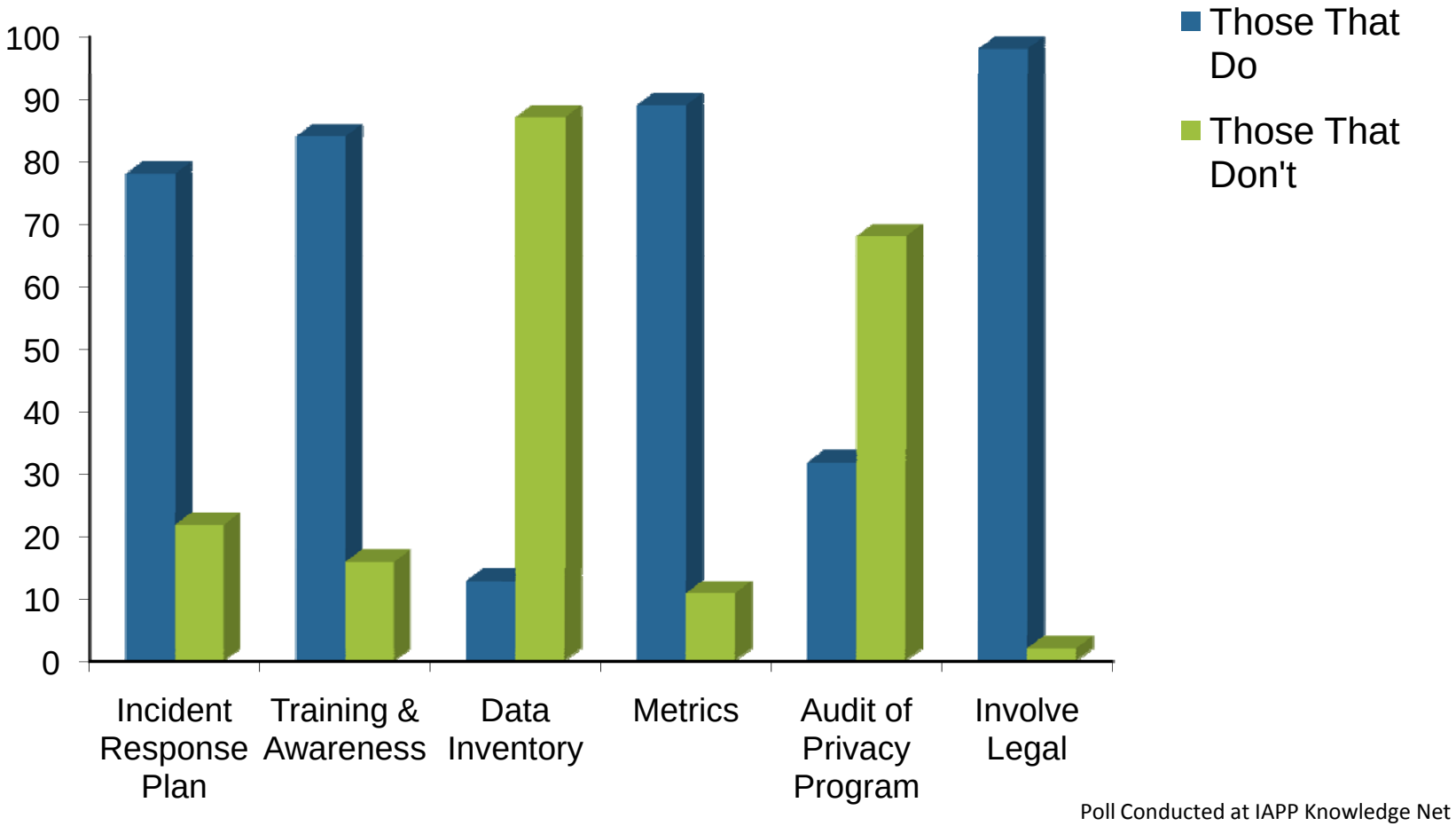
AUDITING THE PRIVACY PROGRAM

- Education of the Audit Team may be helpful
  - May not have solid and detailed knowledge
  - Privacy is relatively new - Landscape changes daily
- Agree upon what is in scope
  - And timeframe – critical when your Privacy program is still "under construction"
- What is the baseline to conduct the Audit?
  - Is it Corporate Policies?
  - Safe Harbor Guidelines
- Leverage the opportunity to use Audit to your advantage
  - How can you mitigate findings without resources or funding?

RESOURCES

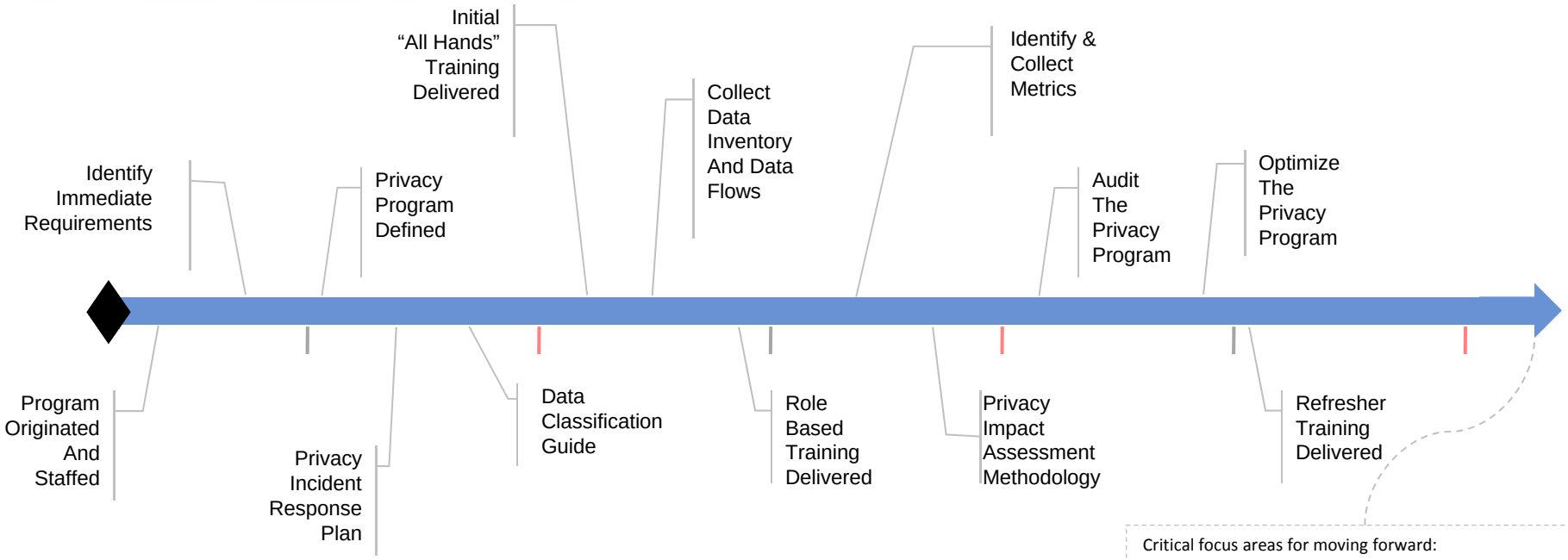
- International Association of Privacy Professionals
  - "Information Privacy" Book
  - Educational events and activities
  - Certified Information Privacy Professional (CIPP) certification
- Institute of Electrical And Electronics Engineers
  - Computer Society's "Security and Privacy" Journal
- Privacy Rights Clearinghouse
  - Numerous Privacy resources, alerts, and news
  - Maintains a chronological and detailed list of Data Breaches
- US Department of Commerce Safe Harbor Site
  - List of all organizations that have self-certified compliance
  - Good Basic Information

WHAT YOU WANT TO BE DOING: WHAT THEY'RE DOING



Poll Conducted at IAPP Knowledge Net Session in New York City, NY 2009

SAMPLE SEQUENCE OF EVENTS



Critical focus areas for moving forward:

- ***Strategy*** – Agree upon a mission, vision and approach.
- ***Program Refresh*** – Review scope and charter, staffing needs, funding, and resource availability.
- ***Management Support*** – Understands the needs and requirements.
- ***Privacy Impact Assessment Remediation*** – Able to track and follow remediation activities .
- ***Tracking and Monitoring*** - Define appropriate metrics to ensure adequate insight and opportunities for improvement.
- ***Enforcement*** – Governance between Risk, Internal Audit, and Information Security, and Privacy.

Each Privacy Program is different, but many of the first steps of deployment are constant.

WHAT YOU CAN DO NOW: EASY WINS

- Privacy doesn't just focus on client data. It affects employees as well. Don't think that you don't need one.
  - Dust off or develop your Privacy Response Plan
- Deliver Privacy Training.
  - Deliver stand-alone or in conjunction with Security Training
  - Get the basics out
- Get involved with some of the Professional Organizations. There are some great resources there!
  - Learn from others doing the same thing that you are
- Find your allies. Build relationships and a 'working council' to help evangelize Privacy in the organization.
- Consider a Privacy Impact Assessment "Lite" to quickly tackle the risks to sensitive information early-on.

CONTACT INFORMATION

George G. McBride, CISM, CISSP, CGEIT
Director of Privacy
Information Technology Shared Services
A Division of Johnson & Johnson Services, Inc.

1003 US Highway 202
Raritan, NJ 08869-0608

Phone: 908.655.3915
Mobile: 732.312.8354
gmcbri32@its.jnj.com