

# Understanding the Importance of Data Privacy

---

**October 2011**

Presented By: Eric Dieterich

## Agenda

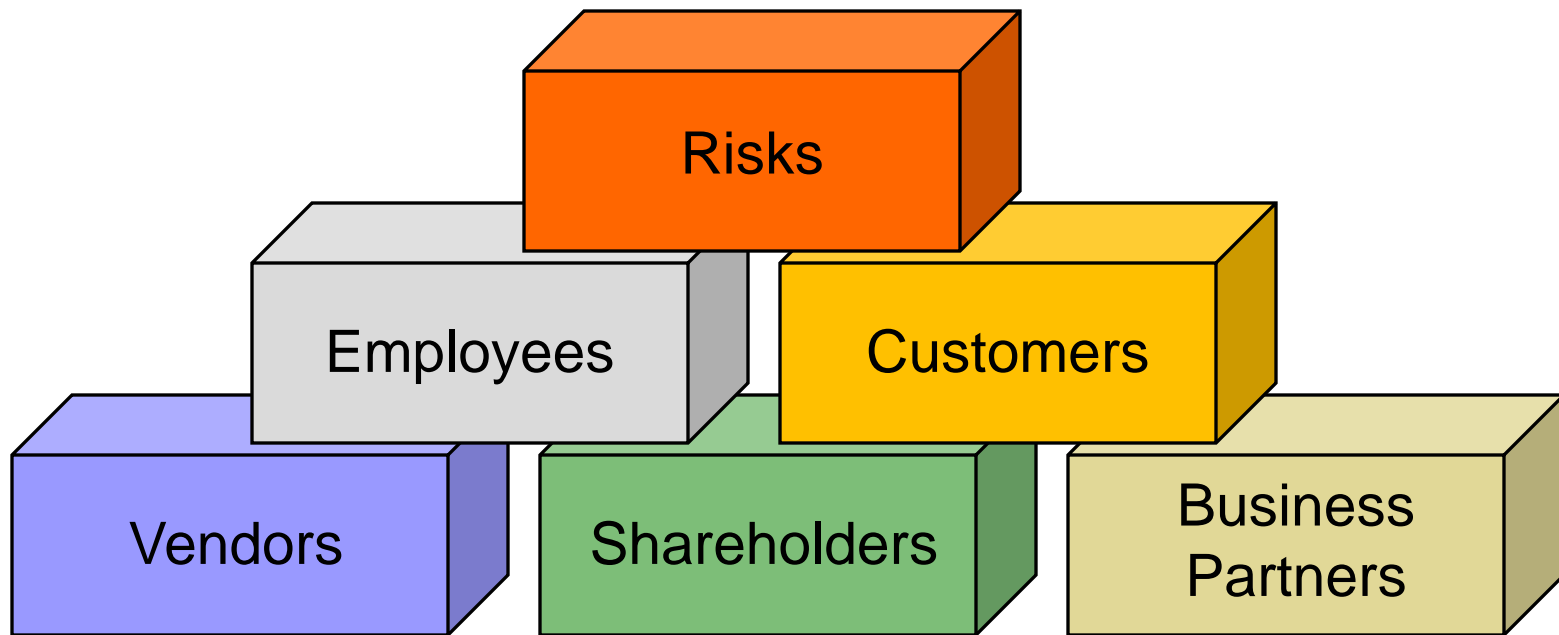
- Why is data privacy important?
- Quantifying the costs of a data breach
- Clarifying the differences between a privacy and security program
- Reviewing current trends with privacy legislation
- Understanding your risk profile and common control failures
- Using a risk based approach to implement a data privacy program

## Why is Data Privacy Important?

- There is a growing body of laws, regulations and legal agreements across the globe that govern how **personal information** should be:
  - Collected
  - Processed
  - Communicated
  - Stored
- A privacy related incident could result in:
  - Regulatory or legal action
  - Direct financial loss
  - Loss of customer or employee confidence
  - Damage to the brand reputation
- For an **individual**, incidents may have the following effects:
  - A mere annoyance at being subject to unwanted direct marketing
  - Being denied a service because of inaccurate data
  - Becoming the victim of identity theft or fraud

## Business Drivers for Data Privacy

- Minimizes risk of compliance breach or regulatory investigation and associated costs.
- Enhances customer and employee trust and builds brand loyalty.
- Protects shareholder and business partner investments.
- Growing awareness of both the public and board of directors.



## Privacy Risk

- The risk associated with privacy and the protection of personal information revolves around the inappropriate or unauthorized **collection**, **use**, **retention**, and **disclosure** of personal information
- The four privacy risks to be considered when determining the overall business risk include:
  - (1) Legal
  - (2) Reputation
  - (3) Operational
  - (4) Loss/Benefit

## What Constitutes a Data Breach?

- Lost or stolen hardware
- Backup tapes lost in transit
- Employees stealing information or allowing access to information
- Poor business practices (i.e. mishandling of sensitive information)
- Careless disposal of information (i.e. exposed via dumpster diving)
- Malware
- A malicious attacker compromising an organization's technical infrastructure

## Recent Data Breaches – A Common Occurrence

### ■ May, 2010 – Aetna Inc. (Connecticut)

- Eight garbage bags filled with names, social security numbers, policy benefits, prescription drug information for hundreds of patients were left **on the side of the road** after an employee disposed of a used cabinet.

### ■ May, 2010 – New Mexico Human Services Department (New Mexico)

- A laptop computer was stolen from a plan providers subcontractors car on March 20<sup>th</sup>. While the computer was password protected it had no other encryption to protect the **9,600 members** of the New Mexico Human Services Department Medicaid plans who have been affected.

### ■ June, 2010 – Digital River: E-Commerce firm (Minnesota)

- A 19 year old male attempted to **sell 200,000 individuals data** for \$500,000. Digital River and the FBI tracked down the hackers to India whom used a “highly unusual search command” to access the data posed as clients. The firm has since sued the young man to determine how he obtained the data.

## Recent Data Breaches – Interesting Case

### ■ June, 2010 – University of Utah

- An Englewood, CO, insurance company has filed a federal lawsuit contending that it is not responsible for reimbursing the University of Utah for the costs related to a 2008 data breach caused by a third-party service provider.
- Backup tapes were stolen from an employee of a third party storage company (Perpetual Storage) while transporting the disks to an off-site backup location.
- The disks, which contained sensitive **data on 1.7 million patients**, were recovered untouched a few day later.
- The University spent **\$3.3 million** in notification expenses, credit monitoring, phone bank, and other fees.

## Data Breach Implications

### ■ AvMed: Health Insurance Provider

- **Breach Description:** May 2009; two laptops containing around 1.2 million members' records were stolen at the insurer's Gainesville, Fla., headquarters.
- **Cost:** AvMed has agreed to provide **two years of credit** monitoring service for all 1.2 million affected members.

### ■ Life is Good Inc.: Clothing retailer

- **Breach Description:** January 2008; stored personal data on computers without using proper encryption software or access controls. The FTC alleges a hacker was able to attack the company's website and obtain credit card numbers, expiration dates, and security codes of thousands of customers.
- **Cost:** Security program assessment performed by external auditors on bi-annual basis for the next **20 years**.

## Data Breaches – Growing In Number!

Between January 10<sup>th</sup>, 2005 and August 16, 2011

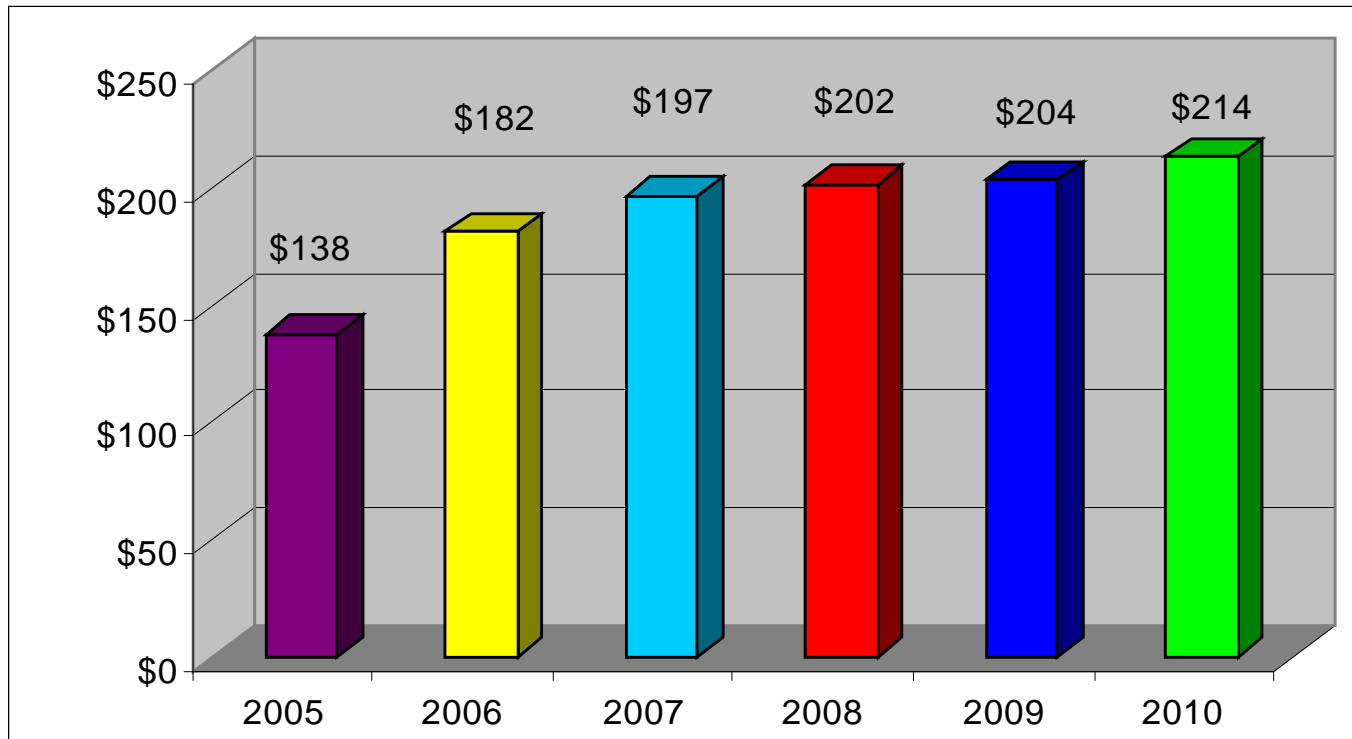
**535,374,400**

records containing “sensitive personal information”  
have been involved in security breaches!

The current U.S.A. population is **311,800,000** in  
mid-2011.

**Source: Privacy Rights Clearinghouse**  
A Chronology of Data Breaches  
Posted April 20, 2005  
Updated August 17, 2011  
[www.privacyrights.org](http://www.privacyrights.org)

## Data Breach Costs Continue to Increase



Source: Ponemon Institute, LLC – “2010 Annual Study: Cost of a Data Breach”

## Breaking Down the Costs of a Data Breach

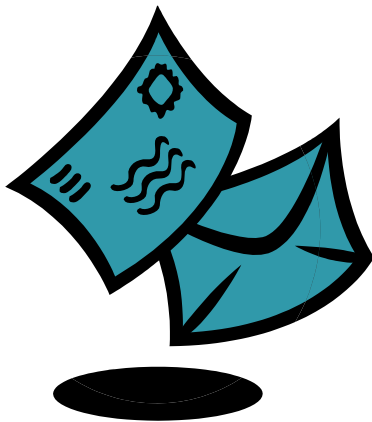
### ■ Cost Estimations – Based on \$214 Per Incident

Cost Per Incident	Records Exposed	Estimated Total Costs
\$214	100	\$21,400
	1,000	\$214,000
	5,000	\$1,070,000
	10,000	\$2,140,000
	15,000	\$3,210,000
	25,000	\$5,350,000
	50,000	\$10,700,000
	100,000	\$21,400,000

### ■ Cost Estimations – Based on \$60 Per Incident

Cost Per Incident	Records Exposed	Estimated Total Costs
\$60	100	\$6,000
	1,000	\$60,000
	5,000	\$300,000
	10,000	\$600,000
	15,000	\$900,000
	25,000	\$1,500,000
	50,000	\$3,000,000
	100,000	\$6,000,000

# Breach Related Expenses



## Notification

- Creating letter or other notification
- Printing or design
- Mailing or other transmission



## Public Relations

- Advertising & Press Releases
- Call Center Operations
- Other Services for Affected Persons:
  - ☞ Credit Monitoring



## Forensics

- Legal Expenses for Outside Attorney
- Cost of Forensic Examination
- Cost To Remediate Discovered Vulnerabilities



## Legal

- Response to Claims or Suits
- Payment of Judgments or Settlements

## Key Privacy Terms

## Clarifying Privacy vs. Security

- The term '**privacy**' often refers to protecting data against various risks, such as the risks of data being accessed or modified by unauthorized persons. However, a more appropriate term for this concept is 'data security' or 'data transmission security'.
- **Security is the protection of information.**
  - Who has access
  - What is most sensitive
  - Who can manipulate the data
- **Privacy relates to the appropriate use of information as defined by:**
  - Laws
  - Circumstance
  - Public sensitivity (Cultural Differences)
  - Privacy can only be assured by an adequate security program



## What is Personal Information?

### ■ Personally Identifiable Information (PII)

- PII is considered any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. Some examples include:
  - Full name
  - Social Security number
  - Street address
  - E-mail address
  - Driver's license number
  - Credit card numbers
  
- It is important to note that other data elements may also be considered personally identifiable information if they are **obtained in unique combinations.**

## Data Types

- **Personal data is collected and stored for numerous purposes within an organization.**
  - **Employee Data**
    - Date of Birth, Social Security #, Health Information, Past Job Experiences, Direct Deposit Information, etc.
  - **Customer Information**
    - Name, Address, Date of Birth, Banking Information, Social Security #, Salary, Tax Information, Pay Stubs, Credit Card #, etc.
  - **Vendor (3<sup>rd</sup> Party) Information**
    - Name, Address, Tax ID #, Bank Information, etc.

Corporate Governance

Risk Management

Regulatory Compliance

## Data Privacy Regulations

## Data Privacy – Regulatory Implications

- **Federal, State, and industry specific regulations govern the collection, use, and storage of PII/PHI.**
  - GLBA
  - HIPAA Security and Privacy Rule / HITECH Act
  - State Privacy/Security Regulations
  - State Breach Notification Requirements
  - Payment Card Industry (PCI DSS)

## HIPAA – The HITECH Act Impact!

American Recovery and Reinvestment Act of 2009 (Effective February 2009)

### ■ The HITECH Act amends the HIPAA Privacy Rules as follows:

- Gives individuals the right to obtain access to their PHI in electronic format,
- HIPAA's criminal penalties apply **not only to covered entities but to individual employees of covered entities and business associates, and**
- ***Increases the amount of civil monetary penalties under the HIPAA rules.***

### ■ Penalties

- Where a person "did not know", \$100 - \$50,000 per violation,
- Where there was "reasonable cause" but no willful neglect, \$1,000 - \$50,000 per violation, and
- If there was willful neglect, \$10,000 - \$50,000 per violation. (with a cap of \$1.5 million).

## HIPAA – The HITECH Act Impact!

### ■ Notifications

- Notice to **individuals** must be provided in written or electronic format.
- Notice must be provided to prominent **media outlets** following the discovery of breaches that involved the information of 500 or more individuals.
- If the breach affected more than 500 individuals, notice must also be provided immediately to the **Secretary of Health and Human Services**.
  - HHS will post on website.
  - If **fewer than 500**, keep a **log of breaches and submit annually** to HHS.
- Notice must be provided **60 calendar days** after “discovery”
  - “Discovery” is the first day the breach is “known” or “should reasonably have been known”.
  - Allows for delay if law enforcement is involved.

# Privacy Legislation and Regulations

## US Privacy Laws

- **Massachusetts 201 CMR 17.00: Standards for The Protection of Personal Information**
  - Applies to all persons that own, license, store or maintain personal information about a resident.
  - Establishes minimum standards to be met in connection with the safeguarding of PII contained in both paper and electronic records.
  - Encryption of PII on mobile devices is required under this statute.

# Privacy Legislation and Regulations

## US Privacy Laws

### ■ Nevada Senate Bill 227 - PCI and Encryption Law

- Nevada law requires businesses to use encryption when data storage devices that contain personal information are moved beyond the physical or logical controls of the business, in addition to continuing to require that personal information be encrypted if it is transferred outside the secure system of the business.
- The new law also mandates compliance with the Payment Card Industry Data Security Standard (“PCI DSS”) for businesses that accept payment cards.
- The law applies to organizations doing business in Nevada and provides that compliance will shield such businesses from liability for damages from a security breach.

## State Breach Notification Laws

- **47 states** plus Washington DC have passed breach notification legislation which require organizations to notify data subjects when a breach has taken place.
- State breach notification laws often require that a government agency (attorney general or a state appointed privacy commission) and/or credit agencies **be notified of the data breach**.

Data Elements Specified in State Breach Regulations		
First Name, or Initial Last Name	Date of Birth Phone Number Address	Digital Signature
Account Number Financial Account Numbers Checking Account Number Savings Account Number	Credit Card Number Credit Card Security Code Debit Card Number PIN	Social Security Number Passport Number
Access Codes Passwords	Biometric Data Fingerprint	Medical Information
Driver's Licence Number State ID Number Non-Driver ID Number	Taxpayer ID Number Federal ID Number Employer ID Number	Parent's Legal Surname Mothers Maiden Name

Corporate Governance

Risk Management

Regulatory Compliance

## International Privacy Regulations

# International Privacy Legislation and Regulations

## Canada Privacy Regulations

### ■ Federal

- **Personal Information Protection and Electronic Documents Act (PIPEDA)** - Applies to the collection, use or disclosure of personal information in the course of any commercial activity within a province. Applies to organizations in provinces other than Alberta, BC and Quebec and to inter-provincial and international personal information transfers.

## European Privacy Regulations

- **European Union (EU) Directive 95/46/EC on the protection of personal information** - In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
- Various legislation by EU member states to enforce the EU Directive.

## Privacy Legislation and Regulations



Country	Do Entities Need to Register?	Comments
Germany	Under Some Circumstances	Registration is not required if the entity has nominated a data protection officer and, either the data subjects have consented to the collection, or the collection serves the purpose of a contractual relationship with the data subject.
Italy	Under Some Circumstances	Notification is required on an exception basis. Registration is required only in cases of particular personal data processing that, in the evaluation of the legislator, presents risks for the data subject (ex. genetic data, DNA, religion).
Spain	Yes	The controller is obliged to communicate the creation of personal data files to the Spanish Data Protection Authority (AEPD).
UK	Yes	If a data controller carries out more than a small range of processing, that controller must notify the processing to the Office of the <i>Information Commissioner</i> . The notified details will be put onto a public register.

## Cross Border Data Transfers

- Regulations around cross border data transfers for multi-national organizations can create unique and complex challenges.
- Options for cross border compliance include:
  - **US Safe Harbor:**  
Set of privacy principles created by the DOC in cooperation with the EU Commission.
  - **Model Contracts:**  
Contracts between the legal entities within a multinational organization.
  - **Binding Corporate Rules:**  
A set of rules, procedures and policies with legally enforceable penalties for non compliance.



## Identifying & Managing Your Privacy Risk

# Data Privacy – Organizational Impact

## ■ Defining

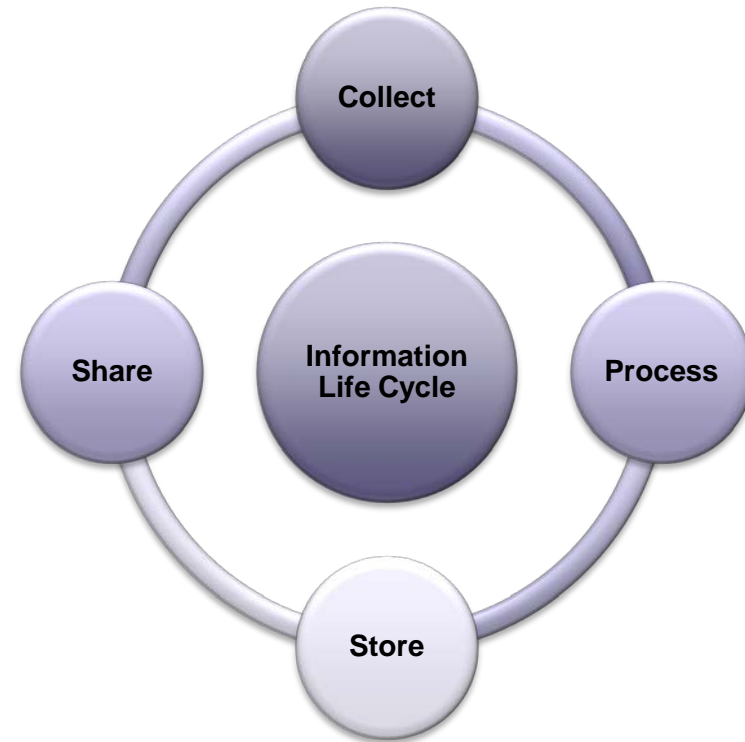
- A data privacy program establishes a framework for controlling how Personally Identifiable Information (PII) is collected, processed, stored, and shared throughout an organization.

## ■ Importance

- Enables an organization to implement policies, procedures, and controls that will reduce the complexities, risks, and costs associated with PII.

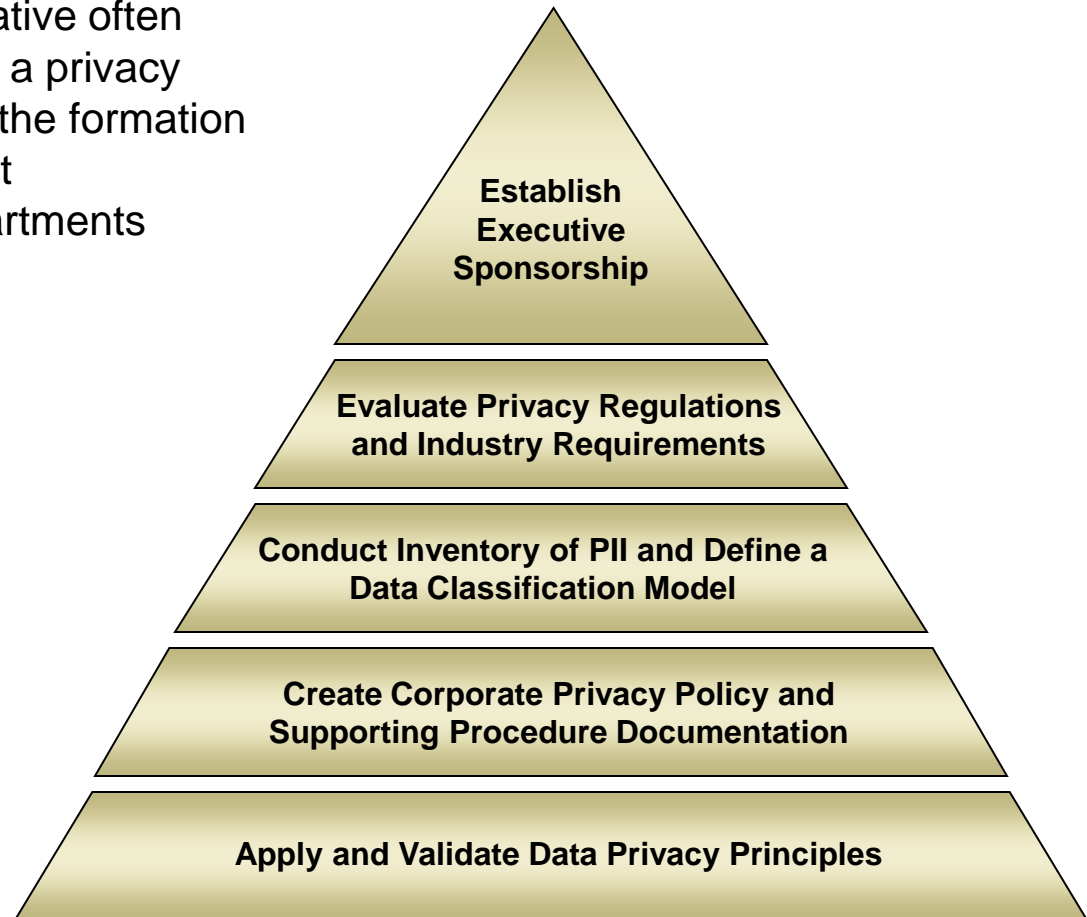
## ■ Strategy

- The foundation of a data privacy program is an organization’s understanding of **how and where information flows through all business processes**. With this knowledge, a framework can be established to **ensure PII is protected throughout the information life cycle**.



## Data Privacy Governance Framework

- Obtaining executive sponsorship at the start of a data privacy initiative often determines the success of a privacy program. We recommend the formation of a privacy committee that encompasses all key departments within the organization.



## Data Privacy Principles

- Data Privacy principles are often defined by industry or country specific privacy regulations and can provide the **framework** for a data privacy program.
- Example data privacy principles include:
  - **Management:** The organization defines documents, communicates, and assigns accountability for its privacy policies and procedures.
  - **Notice:** The organization provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
  - **Choice and Consent:** The organization describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
  - **Collection:** The organization collects personal information only for the purposes identified in the notice.

## Conducting an Inventory of PII / PHI

- With an understanding of compliance requirements, the next step is to determine the sensitive and personally identifiable information (PII) that is:
  - collected,
  - the method of data collection,
  - where it is being stored, and
  - what it is being used for once the initial transaction has been completed.
- We typically collect this information through a combination of:
  - interviews with process owners,
  - surveys, and/or
  - automated discovery tools for high-risk business areas.
- Identified data elements should be classified into different risk categories or classification types in order to determine the privacy risk associated with each data type.

# Conducting an Inventory of PII / PHI (cont.)

## Sunera Data Privacy Survey

**Purpose:**

This document outlines a series of questions to help better understand your business processes for collecting and maintaining personally identifiable information ("PII") within the organization. This is a critical piece of the Company's Global Privacy Program and is required to ensure that the Company is adhering to international privacy regulatory requirements.

PII is considered any piece of information which can potentially be used to uniquely identify, contact, or locate an individual. Some examples include: full name, national identification number, telephone number, street address, email address, driver license number, and health information.

**Objective:** To identify the processes by which the privacy of personally identifiable information is collected and disseminated within the Company.

**Instructions:**

1. Fill out the survey.
2. Please contact **Eric Dieterich**, at **786-390-1490** or [edieterich@sunera.com](mailto:edieterich@sunera.com) for clarification of any questions.

### Contact Information

Name: <input type="text"/> *	Company Address Line 1: <input type="text"/>	
Title: <input type="text"/> *	Company Address Line 2: <input type="text"/>	
Department: <input type="text"/> *	City: <input type="text"/>	
E-mail Address: <input type="text"/> *	State/Province: <input type="text"/>	Postal Code: <input type="text"/>
Telephone Number: <input type="text"/> *	Country/Region: <input type="text"/>	

## Conducting an Inventory of PII / PHI (cont.)

<b>Personally Identifiable Information</b>		
(check all that apply):		
<b>Personal Data</b>		
<input type="checkbox"/> First Name	<input type="checkbox"/> Middle Initial	<input type="checkbox"/> Last Name
<input type="checkbox"/> Mailing Address	<input type="checkbox"/> E-mail Address	<input type="checkbox"/> Fax Number
<input type="checkbox"/> Home Phone Number	<input type="checkbox"/> Cell Phone Number	<input type="checkbox"/> Work Phone Number
<b>Credit Card/Financial Data</b>		
<input type="checkbox"/> Credit Card Type	<input type="checkbox"/> Credit Card Number	<input type="checkbox"/> Credit Card Expiry
<input type="checkbox"/> Credit Card Security Code	<input type="checkbox"/> Cardholder Name	<input type="checkbox"/> Bank Account Number
<input type="checkbox"/> Financial Information	<input type="checkbox"/> Salary	<input type="checkbox"/> Bonus
<b>Other Data</b>		
Please include additional PII data not listed above		
2. What method(s) were used to collect the personal information from the above question?	<input type="checkbox"/> Handwritten Form <input type="checkbox"/> Phone <input type="checkbox"/> Website <input type="checkbox"/> Credit Card Swipe	<input type="checkbox"/> Email <input type="checkbox"/> In-Person <input type="checkbox"/> Kiosk <input type="checkbox"/> Other
3. Please list all computer systems that are used to capture, process, or store any employee information that is collected in your business area (Excel, SAP, Lotus Notes, other application, etc.) If Microsoft Word, Excel, or Access is used to collect or store employee information please identify where the files are stored (local workstation, network drive, etc.).	<input type="text"/> <input type="text"/> <input type="text"/>	
4. What are the <b>business purposes</b> for the collection of this personal information (benefits enrollment, payroll processing, regulatory, etc.)? Please describe.	<input type="text"/> <input type="text"/>	

## Conducting an Inventory of PII / PHI (cont.)



### ■ Discovery Tools – Spider (Freeware)

- Spider can be utilized to identify files that may contain PII and PHI.
- Spider scans a collection of files, searching for patterns of numbers or letters that resemble social security numbers or credit card numbers (additional search patterns can be defined).
- Supports most operating systems: Windows 2000/2003/XP, UNIX, Macintosh.
- Supports most file types: .zip, .doc, .xls, .pdf, .txt, .pst (email), .mdb, .html, etc.

### ■ Analyzing data

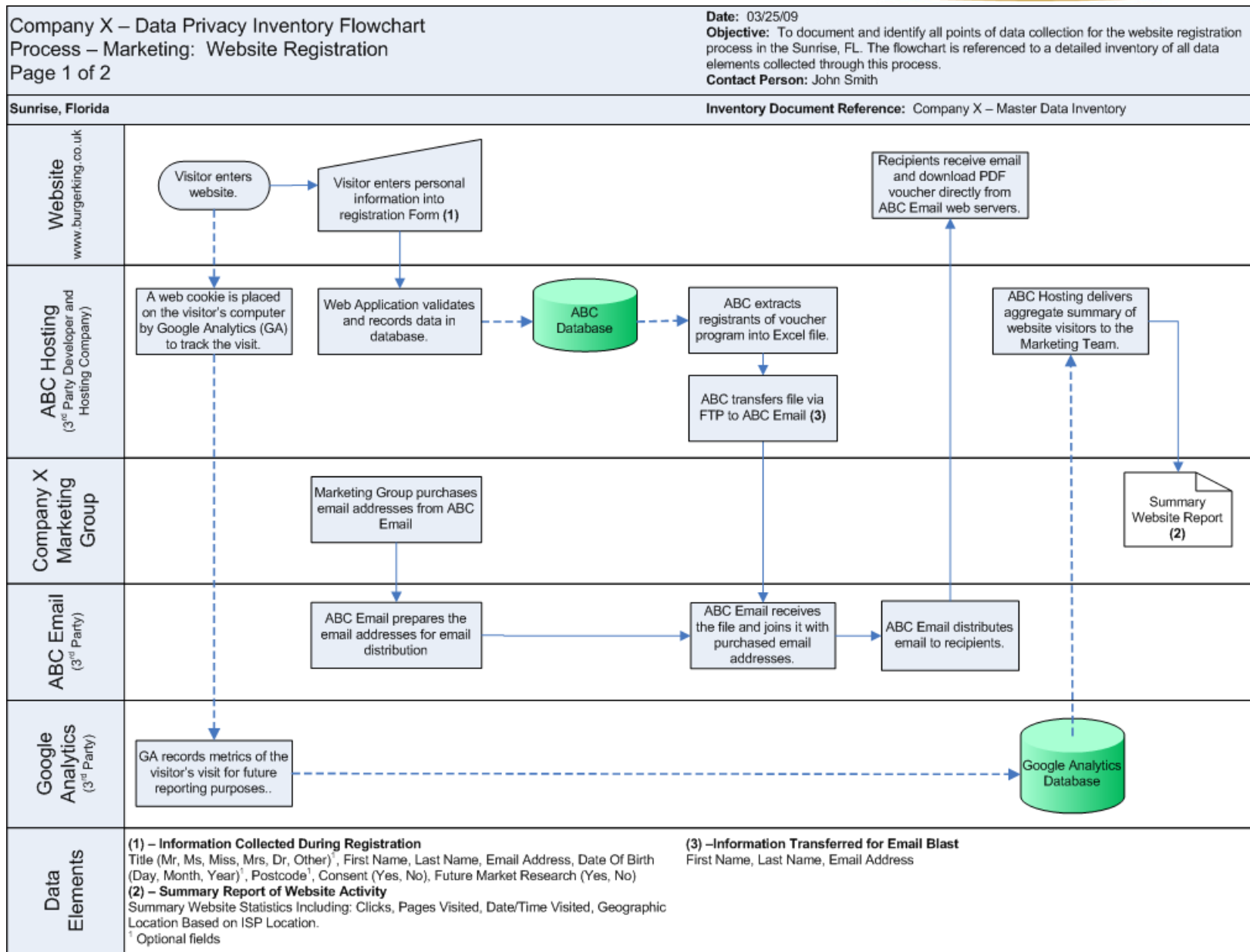
- A log file can be generated (Excel or XML) that lists all the files identified as potentially containing PII or PHI.

HOST	USER	SCAN DATE	PATH	CREATE TIME	MODIFY TIME	ACCESS TIME	REGEX	TOTAL MATCHES
------	------	-----------	------	-------------	-------------	-------------	-------	---------------

- Examine each of the files listed, and take steps to protect any files that prove to contain PII or PHI. Protection steps may include encrypting files, or moving files to a secure server or to offline storage.

## Understanding the Data Flow

- Creating detailed process flows through the discovery process provides many added benefits:
  - Baselines current business operations including data collection and storage practices,
  - Helps identify security and privacy controls,
  - Reduces impact on business operations during future audits and assessments, and
  - When used in combination with a detailed data inventory, it can help identify the scope of a potential breach in an expedient manner.



## Keys to Achieving and Maintaining Compliance –

- Help establish executive management support and prioritization of data privacy as a critical business objective.
  - Leverage enterprise risk assessment results and through the identification of critical risks factors related to privacy and security.
- Help define the assignment of privacy responsibilities.
  - Internal Audit, Compliance, Legal, Information Security, or IT.
  - Elements of a privacy framework should be viewed as a compliance function.
  - Resources should be trained in data privacy matters to help ensure new regulations and the risks they pose to your organization are identified and mitigated.
    - GAPP (Generally Accepted Privacy Principles) – AICPA/CICA/IIA/ISACA
    - International Association of Privacy Professionals (IAPP)

## Keys to Achieving and Maintaining Compliance –

- Ensure control owners are clearly defined.
  - Identify who performs the action and who is responsible for oversight, if applicable.
- Establish periodic or automated controls monitoring.
  - Identify potential issues before they result in control failure.
- Perform annual privacy audits.
  - Can be performed by internal audit or compliance function.
  - Third party assessments can be helpful when subject matter expertise is needed.

# Questions?

**Eric Dieterich**

**Director**

Data Privacy Practice

Sunera LLC

(786) 390-1490

[edieterich@sunera.com](mailto:edieterich@sunera.com)



Please also visit us at [www.sunera.com](http://www.sunera.com)