The Unique Alternative to the Big Four®

Crowe

Protecting Data Privacy: A Practical Guide to Managing Risk

September 19, 2007

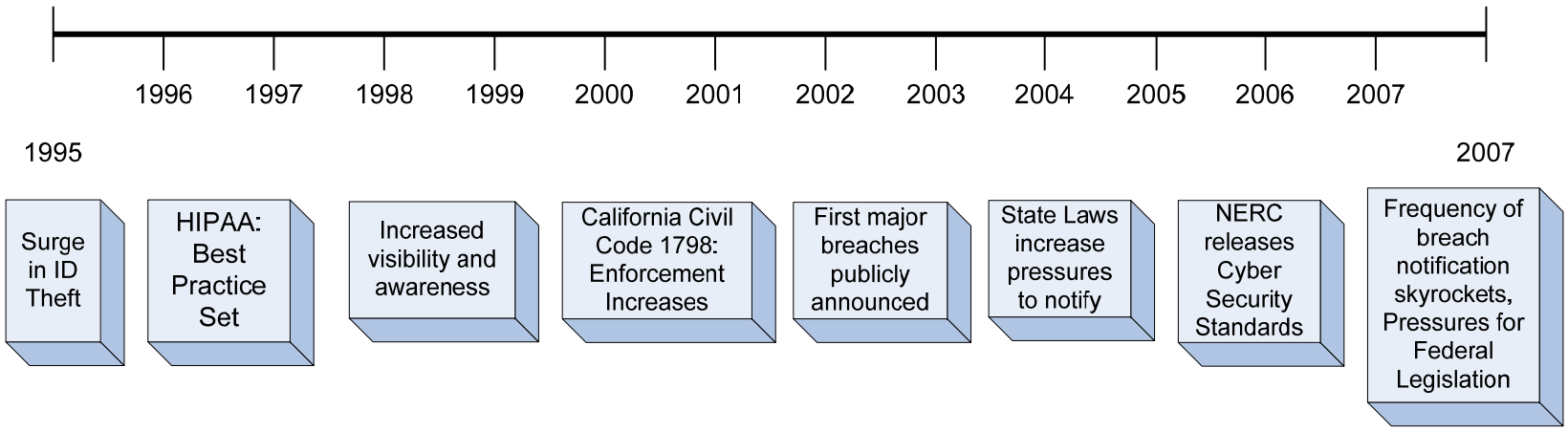
Agenda

- The Goal
- Current Data Privacy Landscape
- Common Privacy Program Pitfalls
- Key Components of a Successful Data Privacy Program
- The Top Down Data Privacy Risk Assessment
- Roles and Responsibilities
- Risk Assessment Results
- High Level Roadmap and Ideas to Consider for Future Strategy

The Goal: Prevent Disclosure

- Understand Legislation, Regulations, Pending Legislation and Best Practices related to Data Privacy
- Assemble a privacy program that is practical, yet effective
- Conduct an assessment to understand risks
  - Identification and Inventory of Data
    - Systems
    - Files/Forms
    - Magnetic Media
  - Classification of Data
    - What is and is not Personally Identifiable Information?
- Educate staff on privacy and information security
- Implement controls that are reasonable
- Mitigate reputation, regulatory, litigation, and financial risks

Current Landscape



Current Landscape: Numerous Breaches

- Bank of America – Backup Tape lost
  - Bank of America Corp. lost computer data tapes containing personal information on up to 1.2 million federal employees, including some members of the U.S. Senate.
- Veterans Administration – Laptop stolen
  - A laptop containing sensitive data including names, Social Security numbers, dates of birth and in many cases phone numbers and addresses, was stolen from a VA employee's home.
- State of Indiana - Website hacked
  - A hacker gained access to the State Web site and obtained credit card numbers of individuals who had used the site's online services and gained access to Social Security numbers for 71,000 health-care workers.
- State of Ohio
  - A backup computer storage device with the names and Social Security numbers of every state worker was stolen out of a state intern's car
- For more stories like this go to:
  - http://www.privacyrights.org/ar/ChronDataBreaches.htm

Current Landscape: Laws for Customer Notification

- Highest profile regulations/laws in privacy environment
- Significant reputational risk impact, potential financial and legal impacts
- Over 35 State Laws – all differ as to the liability, the instances in which notification is required, the types of data considered nonpublic, etc.
- Four pending Federal Bills

Current Landscape – Costs of a Breach

- Ponemon Institute Study (October 2006) found that the total cost of a data breach averaged $182 per lost customer record
  - Direct incremental costs - $54/record
    - Includes discounts, notification letters and legal fees,
  - Lost employee productivity costs - $30/record
  - Customer opportunity costs - $98/record
    - Includes cost of lost customers and cost of acquiring new customers.

Common Privacy Program Pitfalls

- The “Hands Off” Approach
  - Questionnaires and online forms that are “self service” and auto generate recommendations for control improvement.
  - Involving the departments doesn’t mean eliminating the involvement of those with Information Security Expertise
  - Causes frustration amongst departments instead of cooperation

Common Privacy Program Pitfalls, cont

- The inventory of grains of sand at the beach
  - Organizations dive right into databases, looking for fields that are sensitive and should be encrypted
  - Organizations begin scanning systems for patterns of sensitive data without understanding where to expect what.
  - These kinds of activities serve as good follow on steps, but often can cause organizations to become overwhelmed.
  - Most data loss does not occur because of issues at this level.

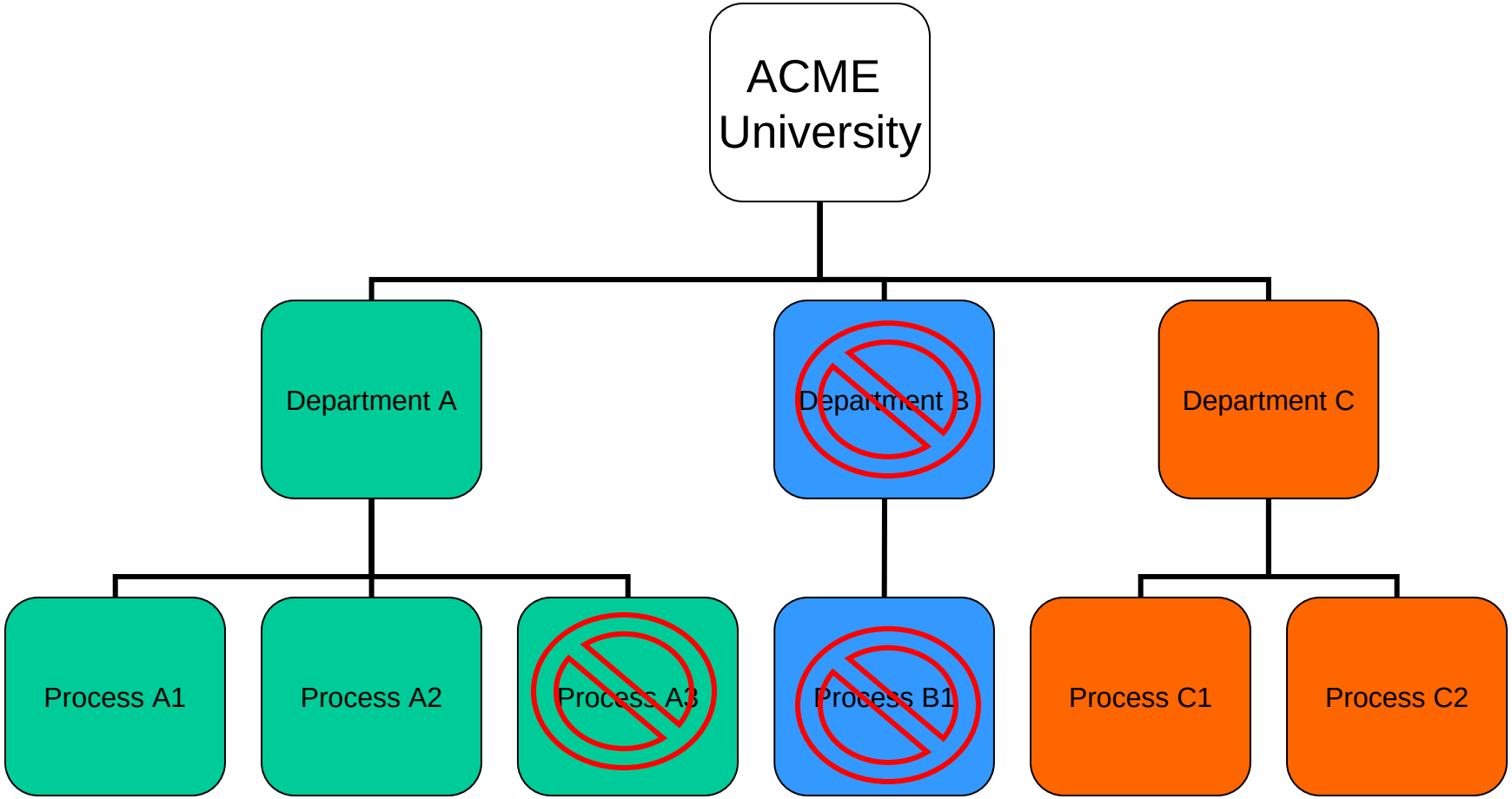
Common Privacy Program Pitfalls, cont.

- Failing to translate risk to an objective level
  - Asking the question “Rank the sensitivity of your data – High Moderate or Low”
  - Asking the question “Rate your controls – Good, Adequate or Poor”
  - Asking the question “Rate the likelihood that this data will be stolen”
  - This is the equivalent of asking someone how tall they are: Tall, Medium Tall, or Medium Short. Instead, you would just ask for their height in inches!
  - You will inevitably find that in the eyes of the owner, data is very sensitive, and very well protected.

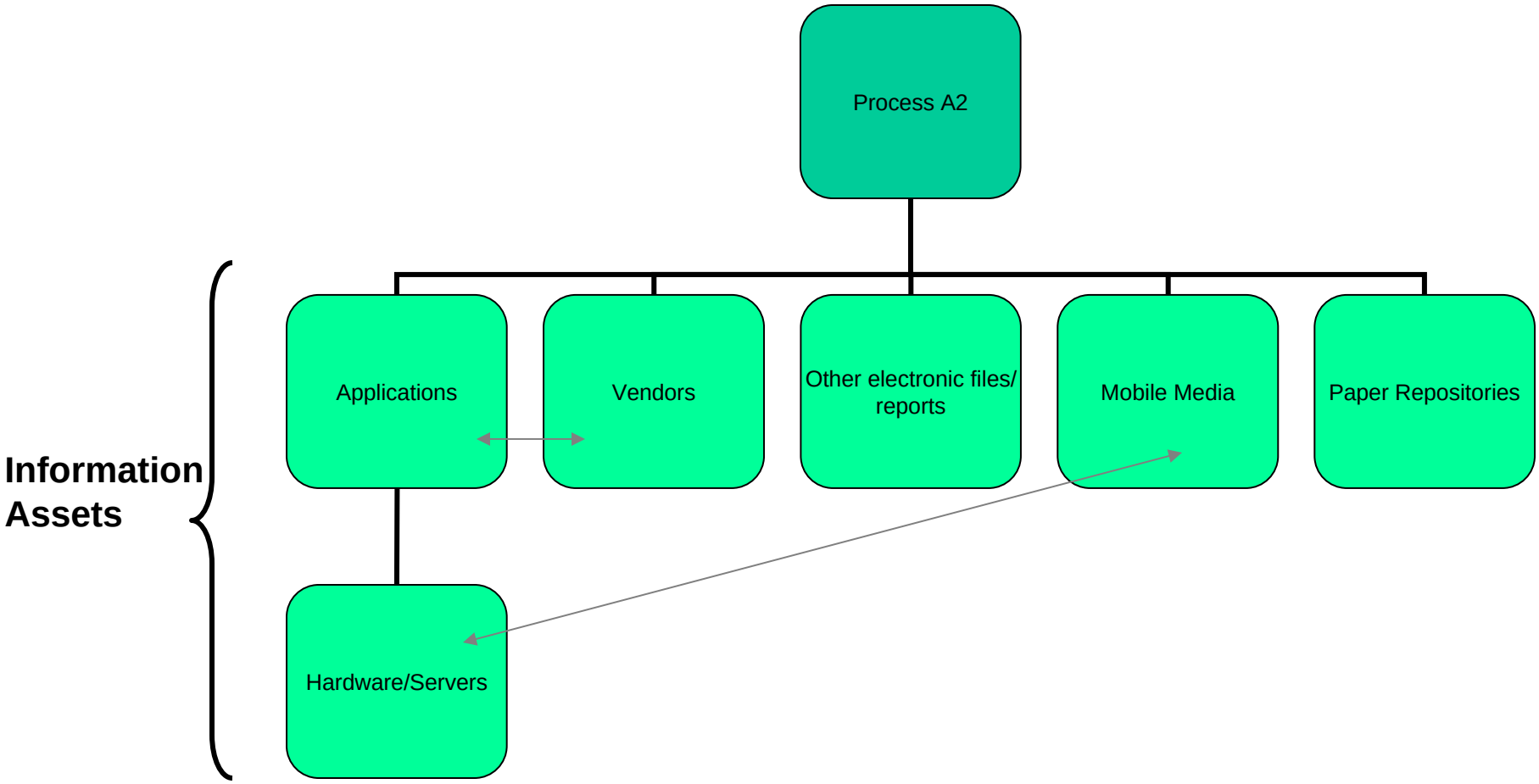
A successful data privacy program…

- Is aligned with the organization's strategic objectives;
- Has the full and visible support of senior leadership;
- Starts at the top of the organization and permeates all business units, divisions, and departments;
- Is championed and managed by individuals with sufficient expertise in information and IT security;
- Is effectively communicated to all employees;
- Is actively monitored and tested for effectiveness.

The Basics of the Top-Down Approach



The Basics of the Top Down Approach, cont.



Overall Approach: Phased Data Gathering

- Step One: Identification of Departments and discussion of Processes and their applicability
  - Information Security expert determines how each uses consumer data in its role in the organization
- Step Two: Inventory of "Information Assets" associated with each process
  - Applications
  - Paper Documents
  - Media
  - Can be classified as is most appropriate
- Step Three : Sensitivity Analysis
  - Determination of the volume and type of consumer data.
  - This should be based on a formal data classification scheme.

Overall Approach: Phased Data Gathering

- Step Four: Control Analysis
  - Each Information Asset should be measured against the control objectives defined for that asset type.
  - Controls can be Physical, Operational or Technical
  - Example: Mobile Media
    - Operational Controls
      - Data is appropriately safeguarded and risks mitigated while media is in transit.
        - Secure electronic transmission is utilized to minimize the media that need to be transported.
        - Media is not stored temporarily or transported in ways that are inappropriate. (ie stored in car trunks, checked in luggage, sent via carrier without tracking capability etc)
      - Media disposal is appropriate.
        - Media is shredded or otherwise destroyed when purged.
    - Technical Controls
      - Encryption controls have been appropriately implemented.
        - Mobile Media has been encrypted prior to transit.

The role of the individual departments

- Provide a comprehensive inventory of applicable information assets on behalf of their department
  - This may involve investigation within their department
- Report accurately regarding the type of data stored as well as the volume of data
- Report accurately about the controls in place to protect this data.
- Ultimately, represent their department in identifying areas where the organization can improve in the protection of consumer data

The role of the Information Security/Privacy Pro

- Establish Information Security Program standards
- Work with each department to understand business processes that affect Consumer data
- Help increase awareness about the risks of poor data safeguarding
- Help everyone understand their role in protecting consumer data
- Review objective data from the Risk Assessment and make educated subjective determinations of risk

The end result

- We know what types of data are stored in what locations, and we've classified this data in a way that is universal.
- We know what types of controls are intended to be in place to protect this data
  - Based on self-assessment, we will need to go back and do validations, audits.
- As such, we can make preliminary determinations of where we have gaps.
  - Gaps are areas where controls are not sufficient given the sensitivity of the data.
- Once a gap is identified, we can work with the business unit to determine:
  - Is the storage of that sensitive data in that place or manner really necessary? Might information be truncated or eliminated?
  - What is an appropriate control that will allow the information to be used but not abused?
- We then track remediation plans to confirm that issues are resolved in a timely manner.

Data Privacy Roadmap: The long term plan

1. Establish a Program Charter
   - Identify objectives
   - Obtain Senior Management Buy In
2. Conduct a Privacy Risk Assessment
   - Top Down Approach
   - Identify Gaps
   - Plan Remediation
3. Establish or Update the Information Security Program
   - Set standards for data protection based on the risk assessment
4. Establish or Update the Incident Response Plan
   - Plan to act timely and appropriately in the event of the worst

Data Privacy Roadmap: The long term plan

5. Test information Security Program effectiveness (and Risk Assessment Accuracy!)
   - Social Engineering
   - Ethical Hacking/External Penetration Testing
   - QA/QC Reviews
   - “Dumpster Diving” or Trash Inspection
6. Build a Sustainable Process for Data Privacy
   - Ongoing awareness and training
   - Ongoing monitoring and testing
   - Periodic environment scan
   - Program modifications as necessary

