

# Sensitive Data Issues

Kerry Digou

# Sensitive Data Cases

Changes in Sensitive Data Cases over the years.

# IANAL

- This is a summary of items and events
- Talk to your GC on how your rules affect you or my rules

# Data Management Policy

- Do you have one?
- Where are you at?

# Kerry's Measure

What's Sensitive Data?

We have PII

We have Policies on PII

We have Standardized  
Tools for PII

We audit our compliance  
with our PII policies

We know where  
all our data is.  
When created it's  
stored appropriately

# Pre-Bethel

- BOR Policy to protect the data
- Limited auditing
- Forensic Investigation for “What broke”

# Bethel

- 4/21/06 - "A hacker accessed names, Social Security numbers, and partial e-mail addresses of current and former students, faculty, and staff."  
<http://www.infosecurityanalysis.com/>
- "A computer server at the Bethel campus of the University of Alaska Fairbanks was breached, university officials said Thursday. Among other information, the server at the Kuskokwim Campus contained two files with nearly 39,000 names, e-mail addresses and Social Security numbers of current and former UA and UAF staff, faculty and students."  
ITRC20060420-03 <http://www.idtheftcenter.org/>

# Bethel Costs

- Notification – Mainly Email
- Call Center – Staff
  - Extended Hours for Support Center
  - After Hours by Data Center
- Bad Publicity
- ASSERT award

# Bethel Changes

- Clean-up
- How to scan for that file and changes to what is in it
- Policy Changes
- Changes to handling compromised machines

# Policies

- Data Management
  - Data Classification in place (08/09)  
[http://www.alaska.edu/records/dataclass/data\\_class\\_std.pdf](http://www.alaska.edu/records/dataclass/data_class_std.pdf)
  - Data Protection is currently in IT review

# Post-Bethel Compromises

- Step 1 – Interview on potential PII data on machine
- Step 2 – Determine likelihood on data compromised
- Step 3 – Present finding to IT/Legal
- Step 4 – Determine whether to notify

# Significant Cases Post-Bethel

- 2006 = 1
- 2007 = 3
- 2008 = 2
- 2009 = 0\*

# Post-Bethel Issues

- Seasonal Data
- Old Data
  - Timesheets
  - Travel Expense Reports
- Old Machine
- Turnaround time

# HB65

- Signed into law 6/13/08 Effective July 1, 2009

"An Act relating to breaches of security involving personal information, credit report and credit score security freezes, protection of social security numbers, care of records, disposal of records, identity theft, credit cards, and debit cards, disclosure of the names and addresses of permanent fund dividend applicants, and to the jurisdiction of the office of administrative hearings; amending Rules 60 and 82, Alaska Rules of Civil Procedure; and providing for an effective date."

# PII Another Definition

- Person's name plus
  - SSN, Driver's license or State Identification number
  - Account Number, CCN, Debit Card Number
    - With password if required
  - Passwords, PINs, or other access numbers for financial accounts

# Notification

- “If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach.”
- Only covers state residents

# Costs

- Notification costs over \$150,000 allow for easier methods.
- Violations can cost:
  - Civil Penalty of \$500/resident
  - Actual economic damages up to \$500 and costs and attorney fees

# Breach of Security

- Does spyware count?
- What if a virus is found on the machine?
- Breach of security is the unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information.

# New Method

- Step 0 – Image the Machine
- Step 1 – Scan the Machine for PII
- Step 2 – Determine if there was a Breach
- Step 3 – Present Finding to IT/Legal
- Step 4 – Notification

# Step 0 – Imaging

- First image the machine
  - Image Masster solo III forensics  
<http://www.ics-iq.com/>
  - Helix
- Hand back the machine

# Step 1 – Scanning

- Scan for PII
  - FIND\_SSN  
[http://security.vt.edu/Find\\_SSNs/index.html](http://security.vt.edu/Find_SSNs/index.html)
  - Spider  
<http://www2.cit.cornell.edu/security/tools/>
  - Identity Finder  
<http://www.identityfinder.com/>

# Step 2 – Breach?

- Very few automatics – Lost laptop, captured traffic
- Factors to consider:
  - Amount of Data
  - Number of Users
  - Elapsed time of Compromise
  - Purpose of Compromise

# Step 2 – Breach?

- Additional Investigation
  - Forensic Investigation of System
  - Netflow Data
  - Interviews

# Step 3 – Determination

- If it was a Breach goto Step 4
- Present findings
  - Encrypted?
  - Amount of Data/Users
  - Length of time
  - Data Transferred non-locally

# Step 4 – Notification

- Advisory role
- Groups Meet – Public Affairs is POC
- Setup teams – Top priority over other jobs
  - Email/Mailing Lists
  - Phone bank
  - Staff Memo
  - Security phone line

# FY 2010 Numbers

- Copyright Cases – 1433 (540)
- CIRT Cases – 174 (102)
- PII Investigations – 52 (52)

# PII Cases

- 52 for FY 10
- This number only includes machines we looked at. Lab machines or student machines are, in general, not looked at.
- Counts are done by number of unique identifiers

# PII Cases Numbers

- 30 Cases with PII Data
- 4 with Substantial amounts
- 1 with Really Substantial amounts

# Non-Evil

- Student folders
- Personal Data – Tax forms, CC/SSN

# Lesser evils

- Personal Tax Forms (not the current user)
- Timesheets
- Travel Coordinators
- Grade Books

# Moderate Evils

- Email
- Images
- DB feeds

# Current Issues

- Time
  - 52 cases last year
  - 5 substantial cases requiring additional work
  - Doesn't cover all forensic work
- Risk
  - Complying with the law
  - Don't want to notify
- IT personnel concerns

# Solutions

- DLP software
  - Less machines to image
  - Less machines with data
- Encryption
  - AS 45.48.010 provides exemption
  - WDE particularly important
- Education

# Questions?