“Responding to Data Breaches”

Jason Pufahl/Chris Misra
Security Professionals Conference
Educause
San Antonio TX
4/5/2011
Introduction

- 14 Years in Information Technology
- 10 Years in Information Security
  - Corporate and Higher-Ed experience
  - Significant Background in Network Security
- I have two jobs
  - Improve security
  - Keep the University out of the paper
    (Certainly Helps with Prioritization)
What is a Breach?
“…unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable…”

Potentially:
- Public Web Content
- Stolen Computers
- Improperly Secured Network Accessible Hosts
- Malware Infected hosts
**What is Personal Information?**

“...personal information“

First name or first initial and last name in combination with any one, or more, of the following data:

(1) Social Security number

(2) driver's license number or state identification card number

(3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.”
Who is Required to Comply?

“Any person that maintains computerized data that includes personal Information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information was, or is reasonably believed to have been accessed by an unauthorized person.”

Considerations:

- How verbose is your logging infrastructure to assist in this determination?
- Determine your organizations ‘reasonable belief’ threshold
- Be consistent
- Don’t be afraid to notify
Some History:

http://datalossdb.org/organizations/121-university-of-connecticut

- 2005 : ~70k Records - Server Intrusion
- 2010 : ~10k Records - Downloaded Report Data
- 2010 : 23 Records – Web Server Posting

All a combination of full name/SSN
President’s Response...

“...I have concluded that UConn must, in the next several months, embark upon a comprehensive and deliberate effort to address computer security concerns. Our focus will be on identifying our vulnerabilities and ameliorating them, both with respect to previously acquired and stored data and data that will be acquired and stored in the future. “

http://security.uconn.edu/?page_id=639

- BOT involvement
- Remove Personally-Identifiable Information (PII).
- Want immediate, tangible results
The “Old?” Days

- Social Security Numbers (SSN) used to be primary ID:
  - Students
  - Posted on walls
  - Key for all systems
    - HR
    - Financials
    - Admissions
    - Purchasing
    - On and on.....
  - PII migrates in from other schools
How We Have Failed?

- Policy Heavy
  - Places responsibilities on data owners
    - We haven’t defined data owners clearly
    - Doesn’t provide any tools for success
- Lack of support at all layers of the institution
- Considered a technology issue
  - Encryption “silver bullet”
  - Spider
- Education
Incident handling still governs the entire process, don’t let an incident that is likely to require notification change your processes

- **Detection**
  - Human processes – Email, Phone, “user clicked something”
  - Training

- **Containment**

- **Classification**
  - This step determines need for Security Breach Team
  - Classification processes continually evolve
  - Don’t look to classify down
  - Don’t be afraid of notification
Proactive PII Program

- **Identity Finder**
  - Site license for Faculty/Staff Students
  - Modules for Web, DB and Email

- **Scan Priorities**
  - Web content priority
  - Application available for download
    - No enforcement, yet
  - User computing devices
  - DB/Email

- **Others Still Relevant**
  - Human processes – Email, Phone, “user clicked something”
  - Training
President declared that PII remediation is a University priority
- Driven by back to back breaches
- Small (23) breach the real catalyst

Internal communications informing community
- Today.uconn.edu
- Town hall meetings
- Email
- TSC
- Deans Council/SAT

External communications
- External Media
Exposures Handling

- **Non Punitive (12-18 Months)**
  - Increase voluntary participation
  - Just solve the problem
  - Notification costs centrally funded

- **Verification**
  - Work with affected areas to validate exposures
  - Decision matrix to assist with decision-making
    - 1. Personally identifying information on publicly-accessible web content
    - 2. Loss\theft of portable devices with unencrypted PII
    - 3. Loss\theft of portable devices with encrypted PII with bad password or exposed password
    - 4. Desktop, laptop, server, or application with PII which has experienced an incident
      - Malware
      - Credentials
      - exploited vulnerability
  - Yes/No/Poor Practice
Notifications

- **Notifications Scheduled**
  - Results collected
  - Results Reviewed bi-weekly
  - Notification process done monthly

- **Debix (Credit Monitoring/ID Theft Protection)**
  - Handles entire process
  - Standardized FAQ/Letters
  - Address verification
  - Question hotline
  - 2 years credit monitoring
  - 1 free credit lift
  - ‘Aftercare’
Opportunities

- Scanning FileLocker periodically to find unencrypted PII – education
- Scanning Exchange – perform from desktop
  - Make sure Console contains information as to where PII was located
  - Education component for departments\users found using Exchange to send PII (for instance, use filelocker)
- File Servers – locate, clean, educate
  - Don’t treat as an exposure
- Figure out a way to catalogue data – where does PII exist
  - Where did it come from? (for example, feeds, reports, etc.)
  - Scan mounted file shares via the desktop rather than the file server to ensure we have a complete inventory
- Finally -

Should a SSN be treated as public information?

Thank you!

Jason Pufahl - CISO
Jason.Pufahl@uconn.edu
security.uconn.edu