



Information Privacy and Security

Security for a New Age

User Services Conference
May 12, 2008

Mike Leach, Project Manager
Jenn Stewart, Technical Coordinator

Objectives

- History of IPAS
- Early stages of Phase II
- Preparing for the Future
- Summary
- Question & Answer Session



History of IPAS

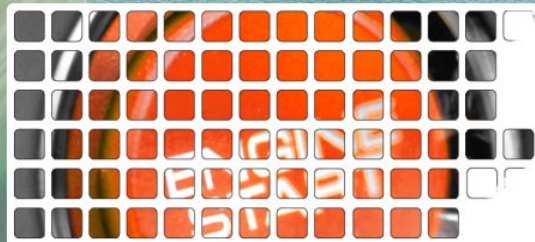
- University-wide Mission
- Formed Fall 2006
- Phase I Goals
- Phase II Goals
- Support and Leadership





Audience Assessment

Responsibilities at PSU



Legal Landscape

Applicable Laws and Regulations (partial):

- **FERPA** (Family Education and Privacy Rights)
- **HIPAA** (Health Insurance Portability Accountability Act)
- **PCI DSS** (Payment Card Industry Data Security Standards)
- The Pennsylvania **Breach of Personal Information Notification Act**
- **FACTA** (Fair and Accurate Credit Transactions Act)



Related PSU Policies

- **FN07** - Credit Card Sales
- **AD11** - University Policy on Confidentiality of Student Records
- **AD19** - Use of Penn State Identifier and Social Security Number
- **AD20** - Computer and Network Security
- **AD22** - Health Insurance Portability and Accountability Act (HIPAA)
- **Trusted Network Specifications**
- **AD35** - University Archives and Records Management



Statistics

- Total Loss of Records to date (2008): 5,557,421
- Over 100 Breaches (2008)
- Approximate Remediation and Notification Cost/record \$197.00

Record Loss Source: Privacy Rights Clearing House

<http://www.privacyrights.org>



Data Breach Examples

1800 Fraud Cases Follow Hannaford's Data Breach

Security breach has **exposed 4.2 million of customers' credit- and debit-card numbers** to scammers, with 1,800 fraud cases reported so far

Breach began Dec. 7, 2007 and continued until March 10 2008



Data Breach Examples

A computer file containing the names and Social Security numbers of current and former Texas A&M University agricultural employees was **inadvertently posted online** and accessible to the public for three weeks.

Total Loss: 3,000

Feb. 16, 2008

Texas A&M University



Data Breach Examples

A university laptop containing archived information and Social Security numbers for 677 students attending Penn State between 1999 and 2004 was recently **stolen from a faculty member.**

Total Loss: 677

Jan. 25, 2008

Penn State University



Online Threats

- Botnets
- Viruses
- Worms
- Spyware
- Other Popular Scams
 - Phishing scams
 - Advertisement banners





Data Classification | File Scanning | Encryption

Early Stages of Phase II

Data Classification

- 2 Primary Classifications of Systems/Networks
 - **Public**
 - **Non-Public**
- 3 Primary Classifications of Data
 - **Public**
 - **Internal/Controlled**
 - **Restricted**
- 10 Security Categories



Personally Identifiable Information (PII)

- Social Security Numbers
- Financial Information
- Credit Card Numbers
- Student Data
- Donor Information
- Legal Council Information
- Personal Health Information

...list not exhaustive



File Scanning

- Goal: Detect sensitive information
- Beta Test with Select Units
- Implementation Fall 2008
- Details to Follow
 - Network of People (Tues, 5/13)
 - Awareness Campaign



Encryption

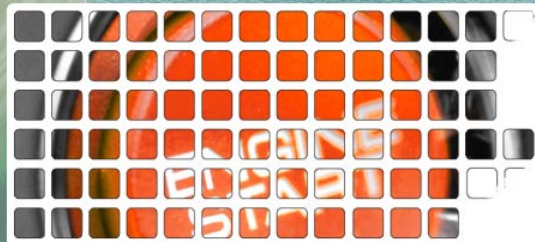
- Software: Utimaco's SafeGuard Easy
- Options: disk drive, mobile device
- Purpose: protect sensitive information
- Target:
 - all mobile devices
 - desktops in open environments
 - desktops processing PII
- Implementation: Fall 2008





Audience Assessment

Who has already starting thinking about file scanning and encryption?





Electronic and Physical Security

Preparing for the Future

Electronic Security Measures

- **Strong Passwords**
 - 7 characters
 - Numeric and alphabetic
 - Change every 90 days
 - Never use names, birthdates, etc.



Electronic Security continued

- Common Sense Security
 - Internet searches
 - Email
- OS and AV Updates
- Administrator Privileges
- Local Policies



Physical Security

- Laptop
 - Security cable
 - Carry-on vs. checked
- Sensitive Paper
 - Locked cabinet
 - Limited access
 - Shred after use



Reporting

- Security Operations and Services (SOS)
 - Suspicious activity
 - Email legitimacy
 - Contact
 - Normal work hrs
814-863-9533
 - After hrs 814-777-9533
 - security@psu.edu



Summary

- Protect the institution
- Protect data being handled
 - Customers, students, donors, etc.
- Meet on-going compliance obligations
- Limit reportable data breaches
- Enhance business practices at Penn State



Resources

- IPAS: www.ipas.psu.edu
- Guru Policies
<http://guru.psu.edu/home.cfm>
- Privacy Rights Clearing House
<http://www.privacyrights.org/index.htm>



Question and Answer Session

Information Privacy and Security (IPAS)

814.867.1340

www.ipas.psu.edu

ipas@psu.edu

