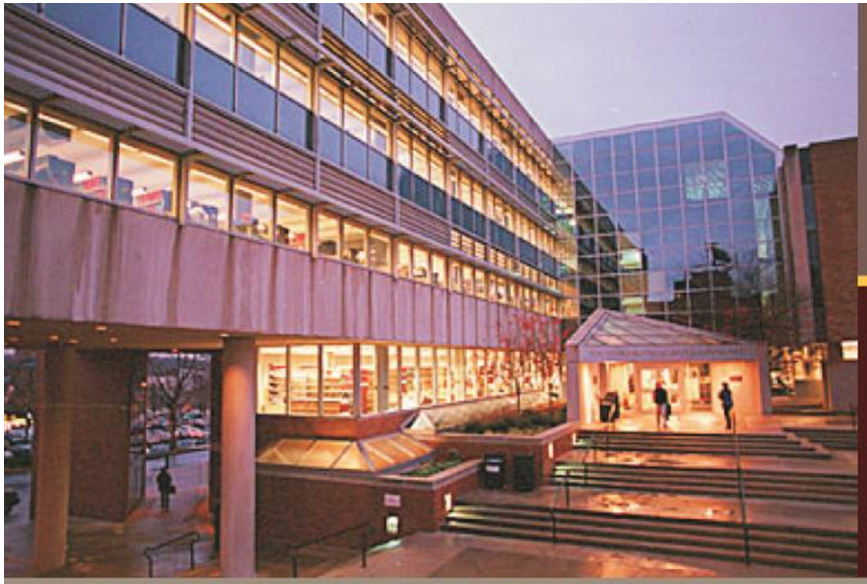


LEHIGH
UNIVERSITY

PGP Whole Disk Encryption Implementation

Educause National Conference
October 29, 2008

Gale Fritsche

Tim Foley

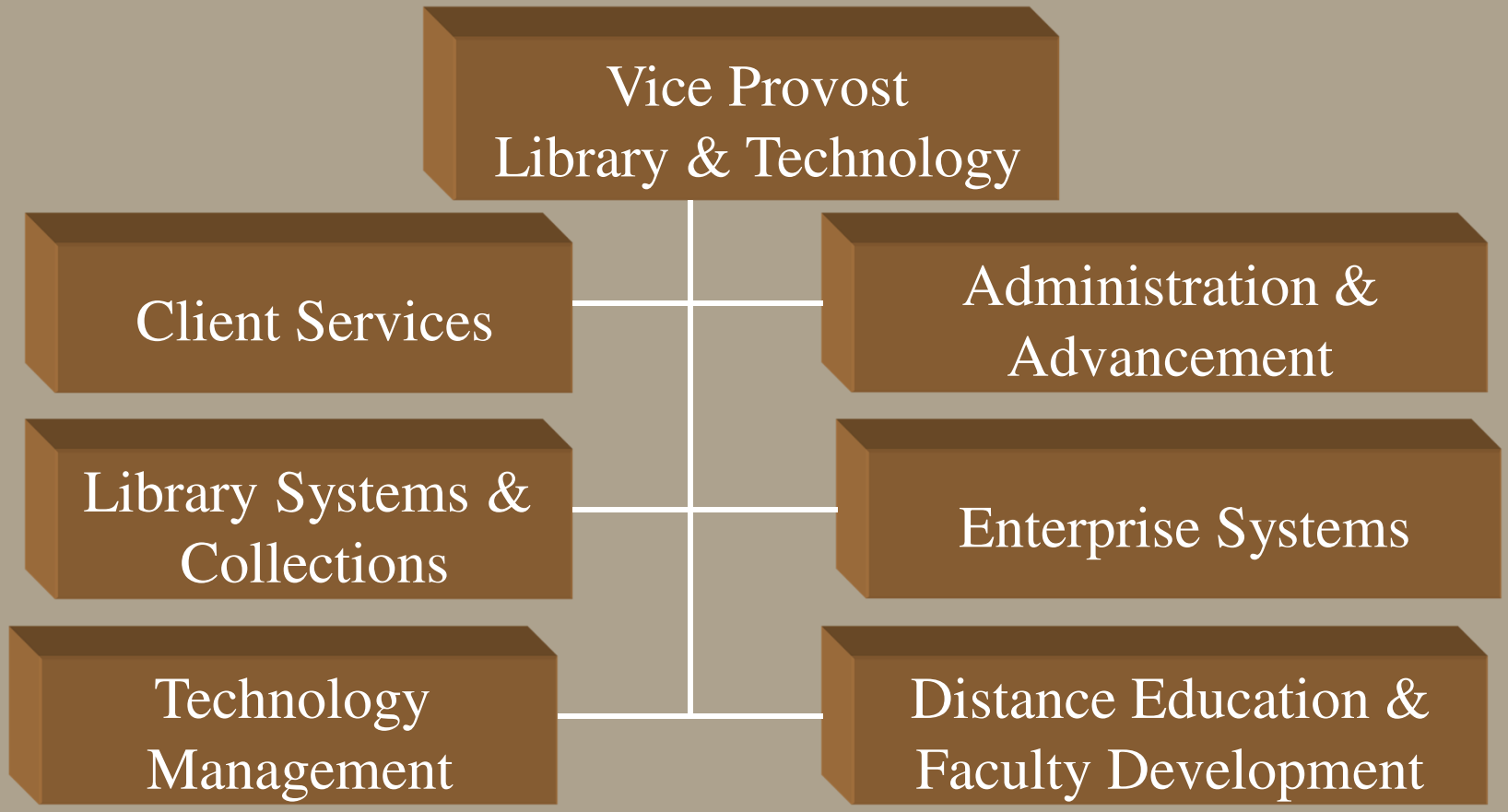
Lehigh University
Library and Technology Services

Lehigh Overview

- Founded in 1865. Private research university located 90 miles west of NYC
- Ranked 35th in US News and World Report 2009 “Guide to America’s Best Colleges.”
- Approx 4700 undergraduates, 1200 graduate students, 450 faculty and 1200 staff
- Approx 80% Windows PCs, 15% Mac and 5% other (Linux etc.)

LEHIGH UNIVERSITY

Library & Technology Services Organizational Structure



LEHIGH UNIVERSITY

Presentation Agenda

- Why Encrypt?
- Lehigh's Committee Structure
- PGP Pilot Program
- PGP Implementation Plan
- Issues and Roadblocks

LEHIGH UNIVERSITY

Why do we need encrypted information in educational institutions?

- University of Iowa College of Engineering - Some students are being notified by the college that their personal information may have been exposed in a recent computer breach. The compromised computer contained a file with names and Social Security numbers of students stored on its hard drive. (Sept 11, 2008)

- Tennessee State University - A flash drive containing the financial information and Social Security numbers of students was reported missing. The flash, which contained financial records of TSU students dating back to 2002**.** (Sept 12, 2008)

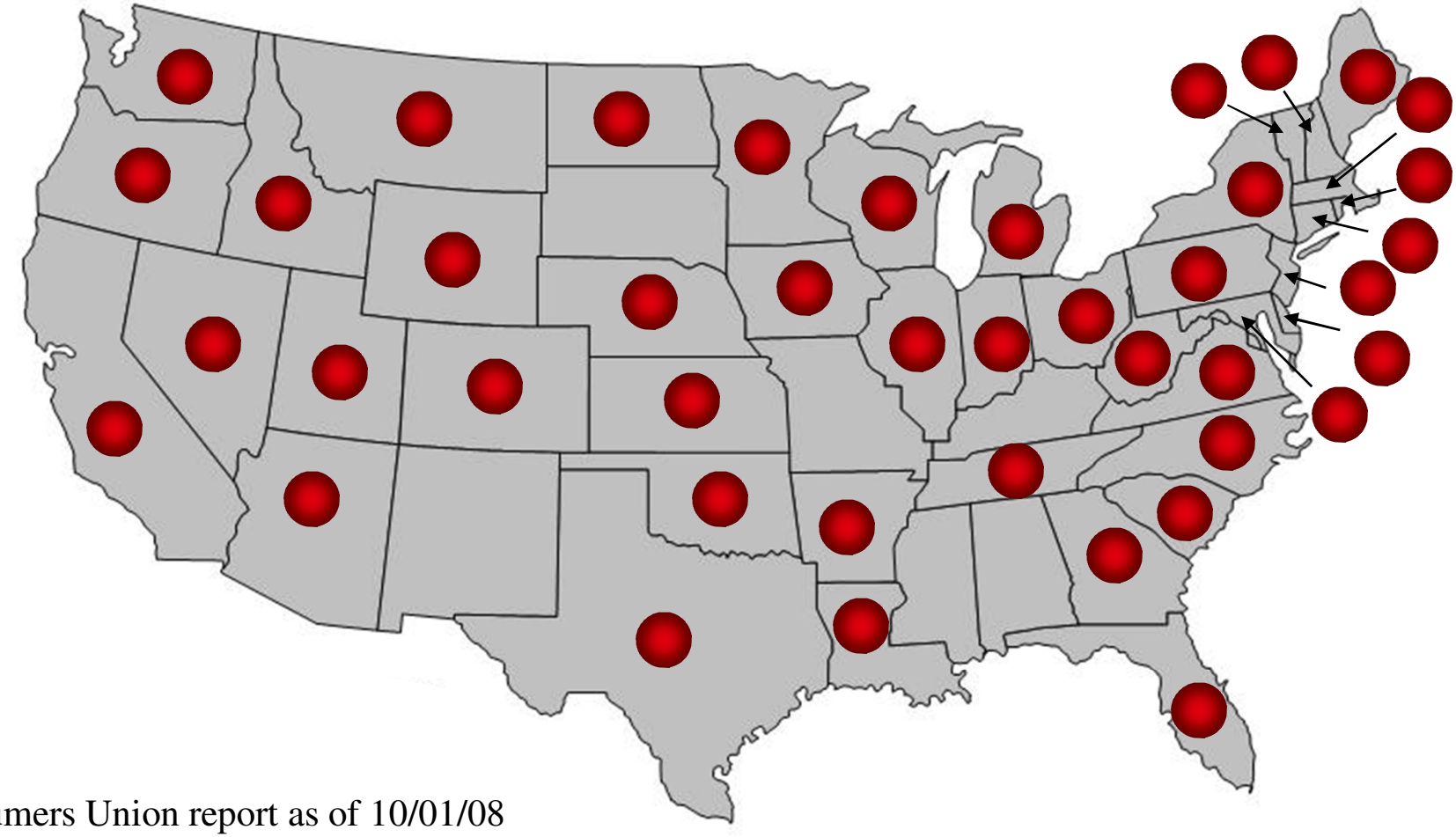
- A hacker attacked the University of Indianapolis' computer system and gained access to personal information and Social Security numbers for 11,000 students, faculty and staff. (Sept 30, 2008).

Source: Privacy Rights Clearinghouse

LEHIGH UNIVERSITY

44 states with security breach laws (as of 10/1/2008)

(Puerto Rico and District of Columbia also have laws)



Consumers Union report as of 10/01/08

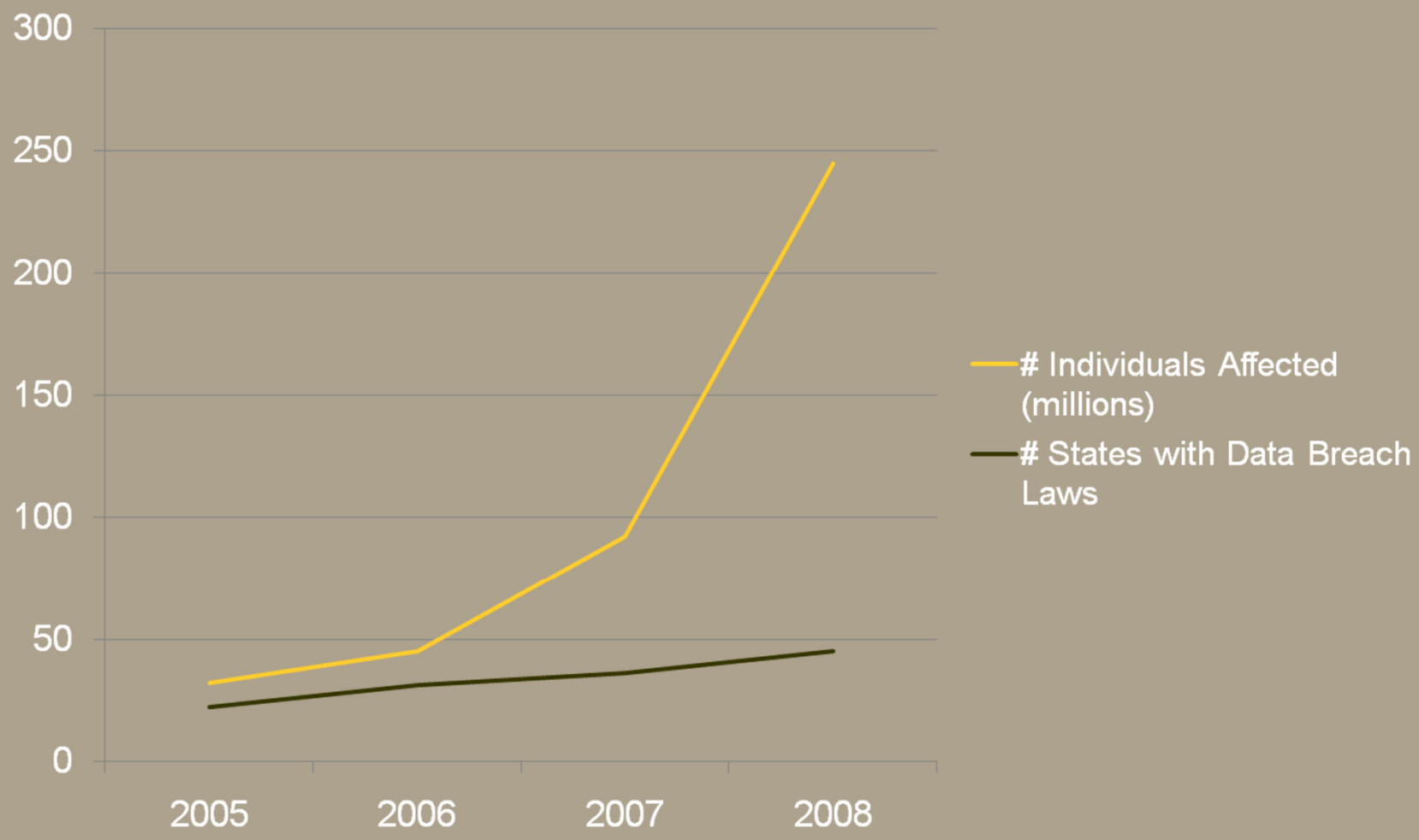
Reported breaches - **245,044,535** people affected since 1/15/05

see: http://www.privacyrights.org/ar/ChronDataBreaches.htm

LEHIGH UNIVERSITY

Growth in number of individuals affected by data breaches

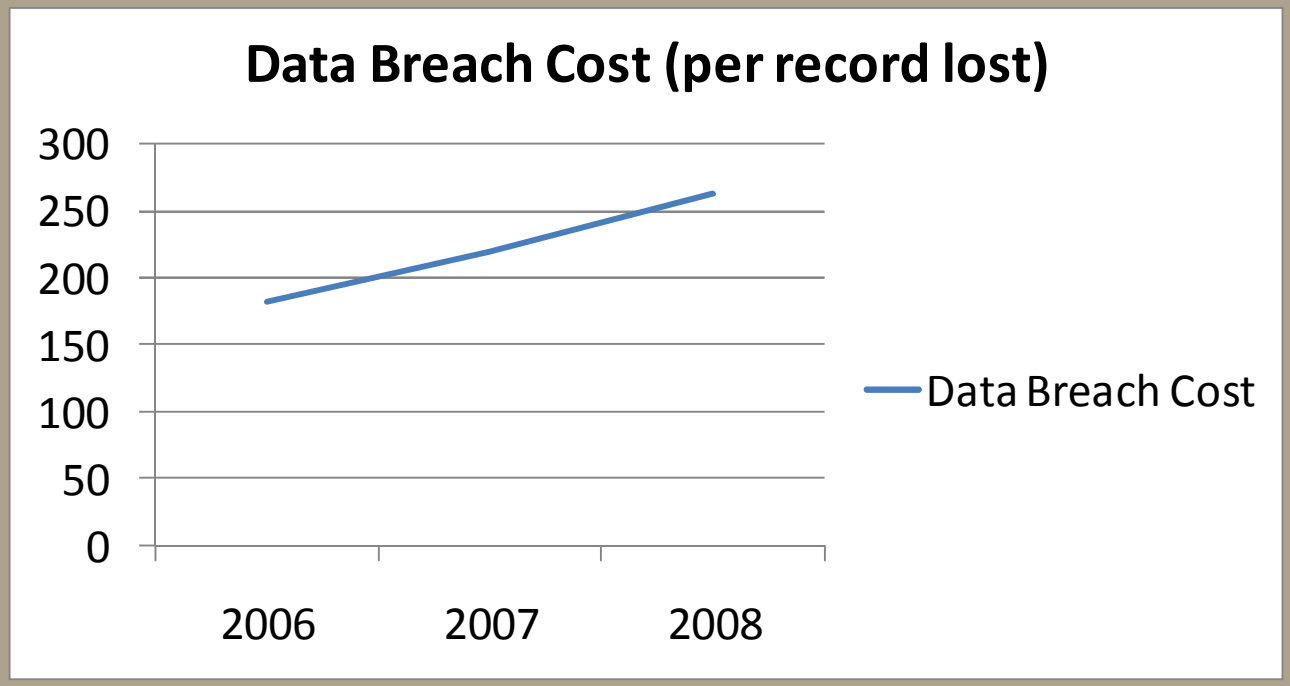
Source: Privacy Rights Clearinghouse 2008



LEHIGH UNIVERSITY

Cost of Data Breaches

Source: Ponemon Institute, LLC

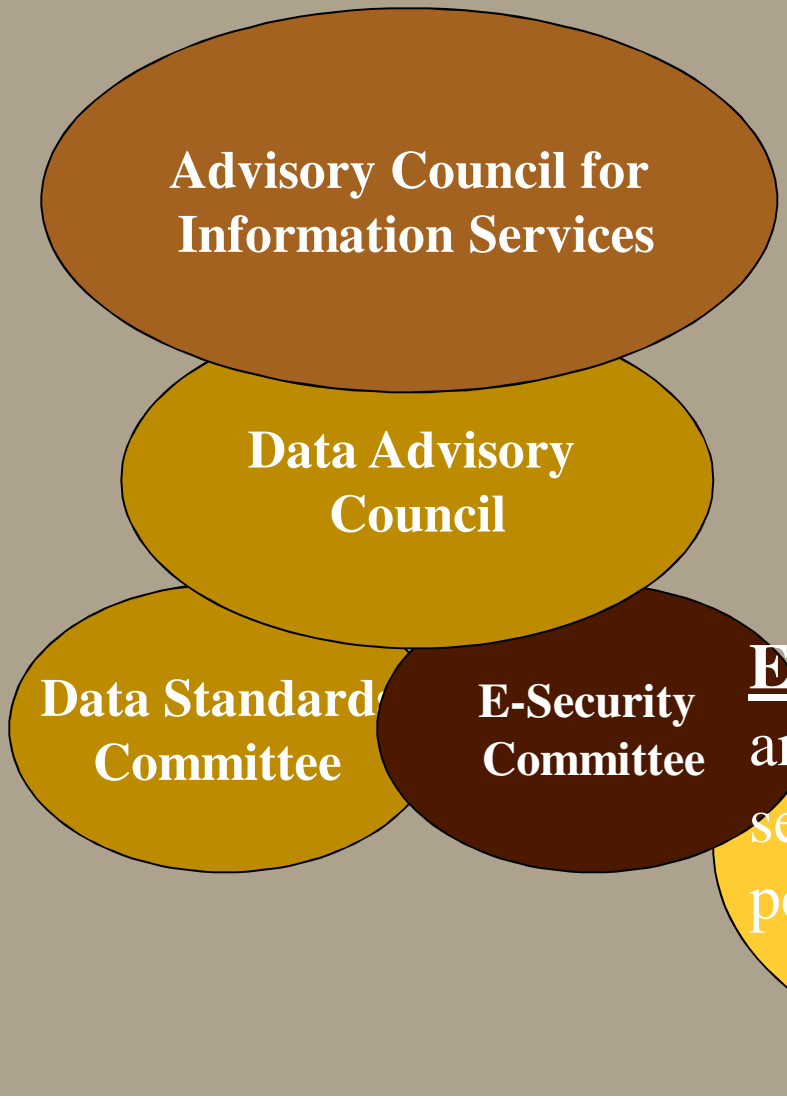


LEHIGH UNIVERSITY

Lehigh's Procedure in Case of a Data Breach

- Security Officer works with technical & legal staff to determine the extent of the problem and if it requires a legal response
- Lehigh technical staff determines the extent of the problem & works to minimize damages – some action taken immediately
- University Communications develops a communications plan – reviewed by risk management and legal counsel – prepare for media inquiries
- Credit monitoring services offered to affected individuals for at least 12 months – cost start around $15 per month
- PA breach law states – name combined with SSN, DLN, or credit card information constitutes a notifiable breach

Committee Structure



Advisory Council for Information Services – sets university wide information services policies

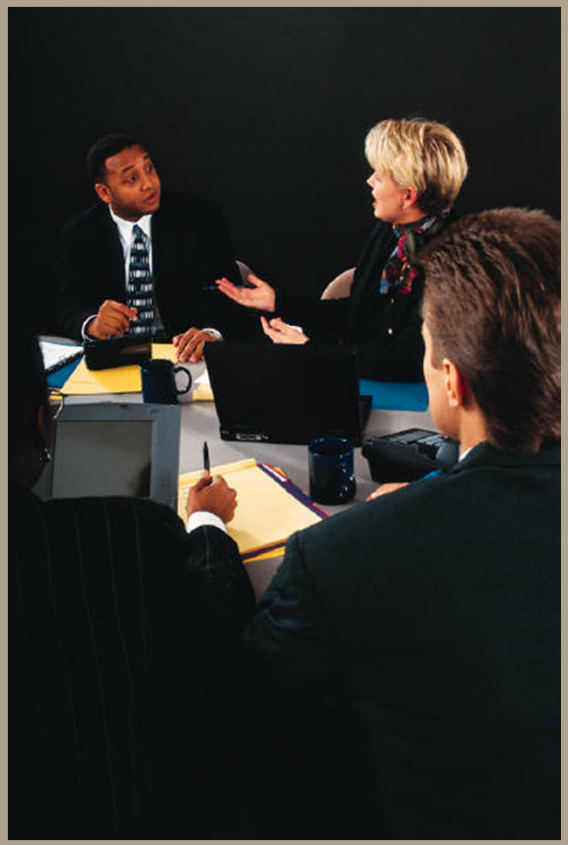
Data Advisory Council – ensures data standards are maintained and enforced

Data Standards Committee – Addresses the best way to encrypt Personal Data and other Sensitive Information on systems, portable devices, and backups

E-Security Committee – Addresses Lehigh's standards for shared data elements in Banner and recommends implementation of security related practices and policies

LEHIGH UNIVERSITY

Data Encryption Committee

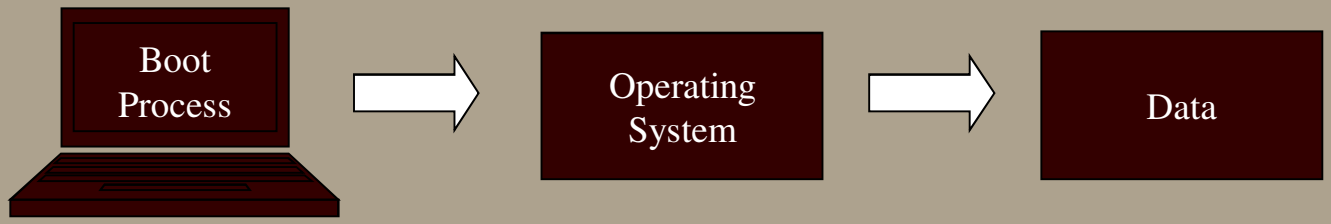


- Looked at various methods of encryption
  - File/folder encryption
  - Container encryption
  - Whole disk encryption
- Determined that whole disk encryption (WDE) was necessary
- Selected products to be tested
- Developed criteria for testing
  - Platform compatibility
  - Performance
  - Ease of Use and Administration
  - Cost

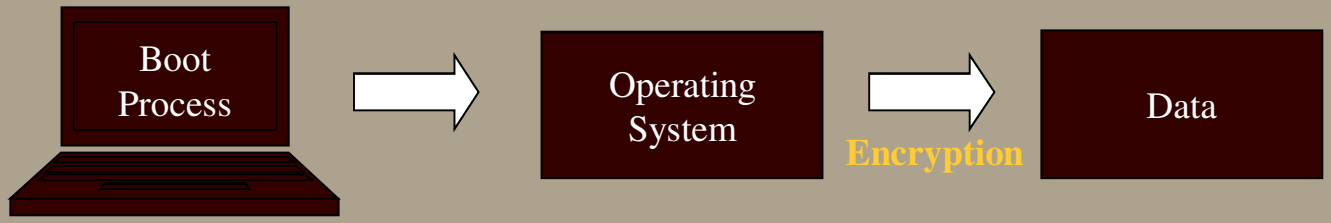
LEHIGH UNIVERSITY

How Whole Disk Encryption Works

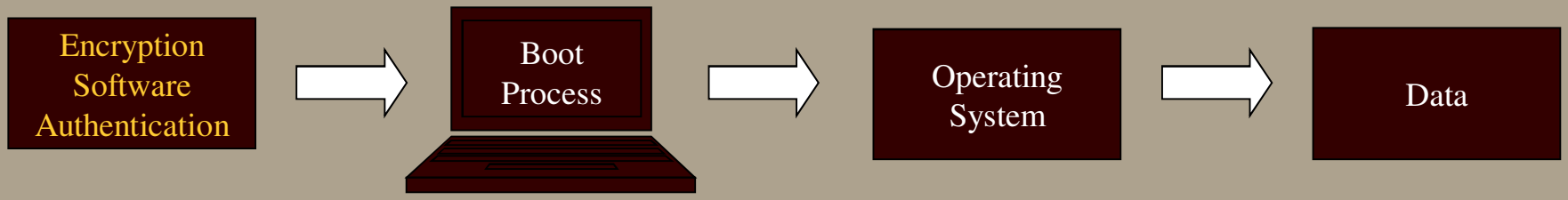
No Encryption



File Encryption

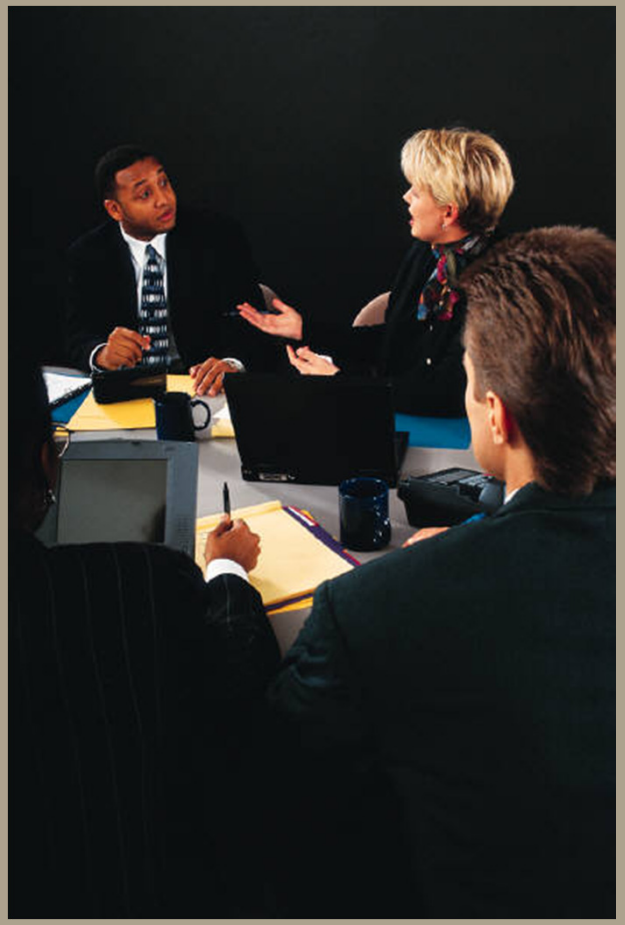


Whole Disk Encryption



LEHIGH UNIVERSITY

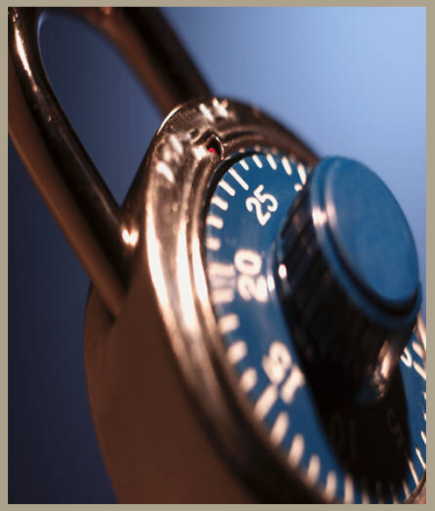
Data Encryption Committee
(Continued)



- Evaluated Products
  - WinMagic (Securedoc 4.2)
  - PGP Desktop Pro 9.0
  - Pointsec 6.0
  - Securstar (DriveCrypt 3.5)
  - Ultimaco (Safeguard 4.2)
- Performed Benchmarks (Performancetest 6.0)
  - CPU
  - Memory
  - Disk Read/Write
- Selected PGP as the product of choice
  - Recommended to encrypt all Faculty/Staff PCs on Campus

LEHIGH UNIVERSITY

Why PGP Desktop and Universal Server?

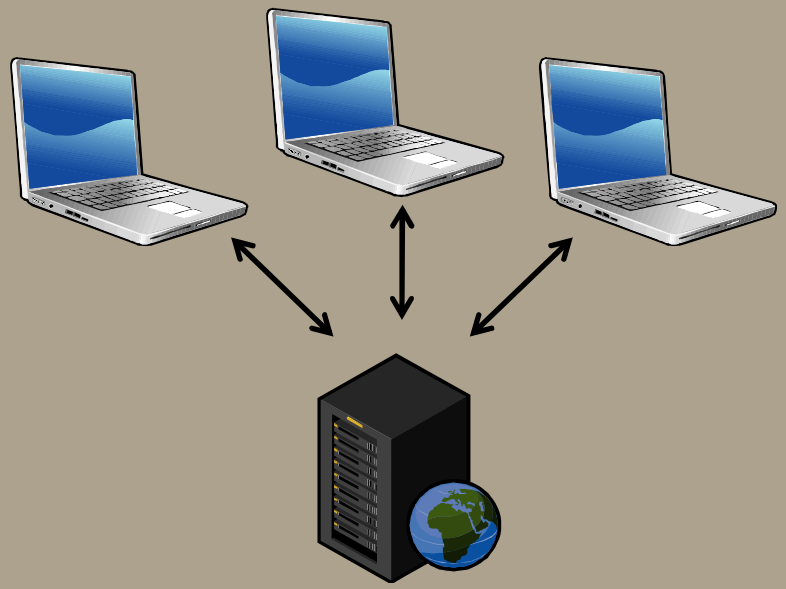


- Desktop Platform Compatibility
  - Macintosh and Windows compatibility (95% of users)
- Limited Hardware Requirements for Server
  - Universal Server installed in a virtual environment
- Limited Server Administration
- Server Policies and Customized Installers
- Integration with Microsoft's Active Directory
- Easy recovery of encryption keys
- Price
  - Educational pricing is 50% off list (PGP Limited)

LEHIGH UNIVERSITY

PGP WDE – A closer look

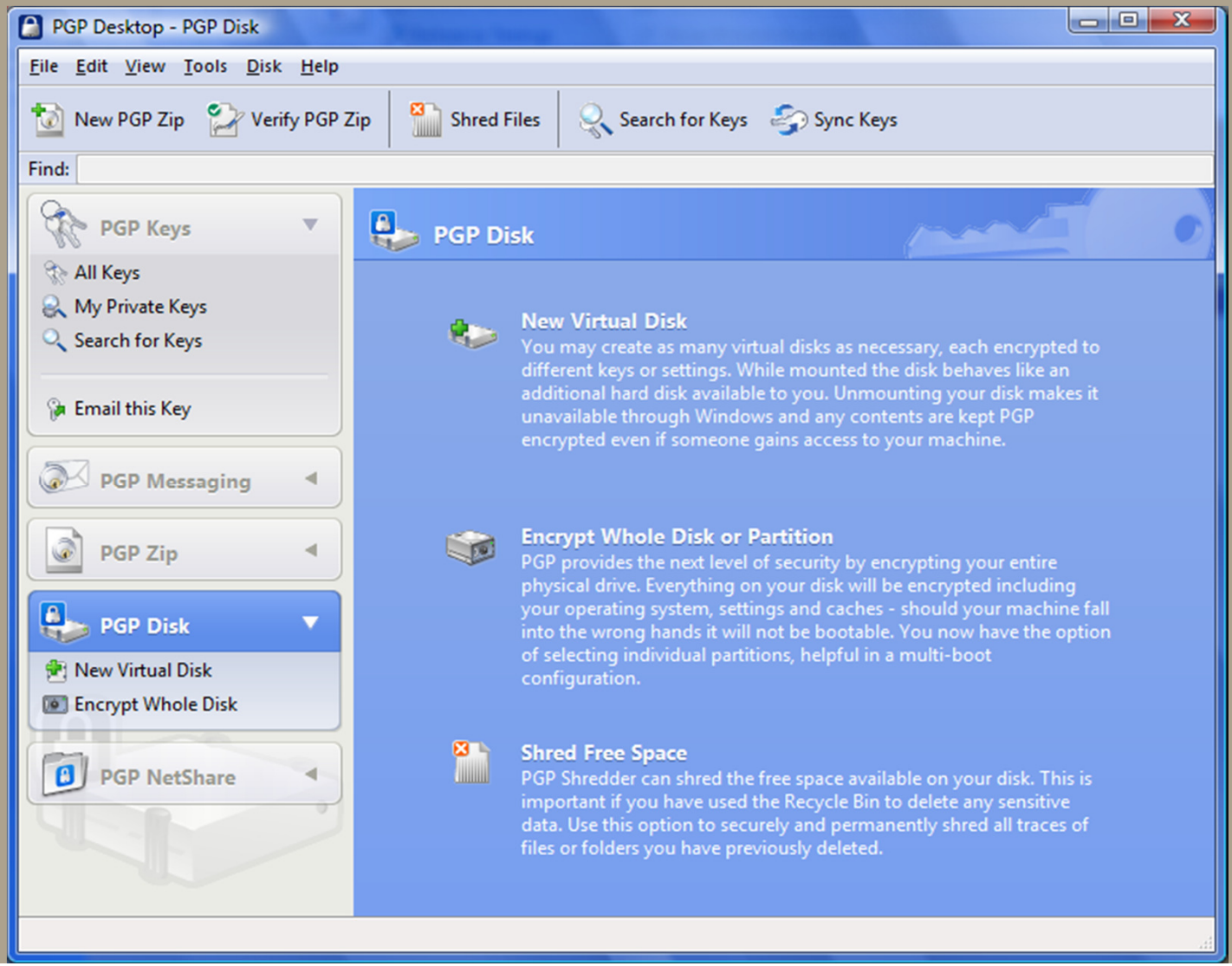
- PGP Desktop



- PGP Universal Server

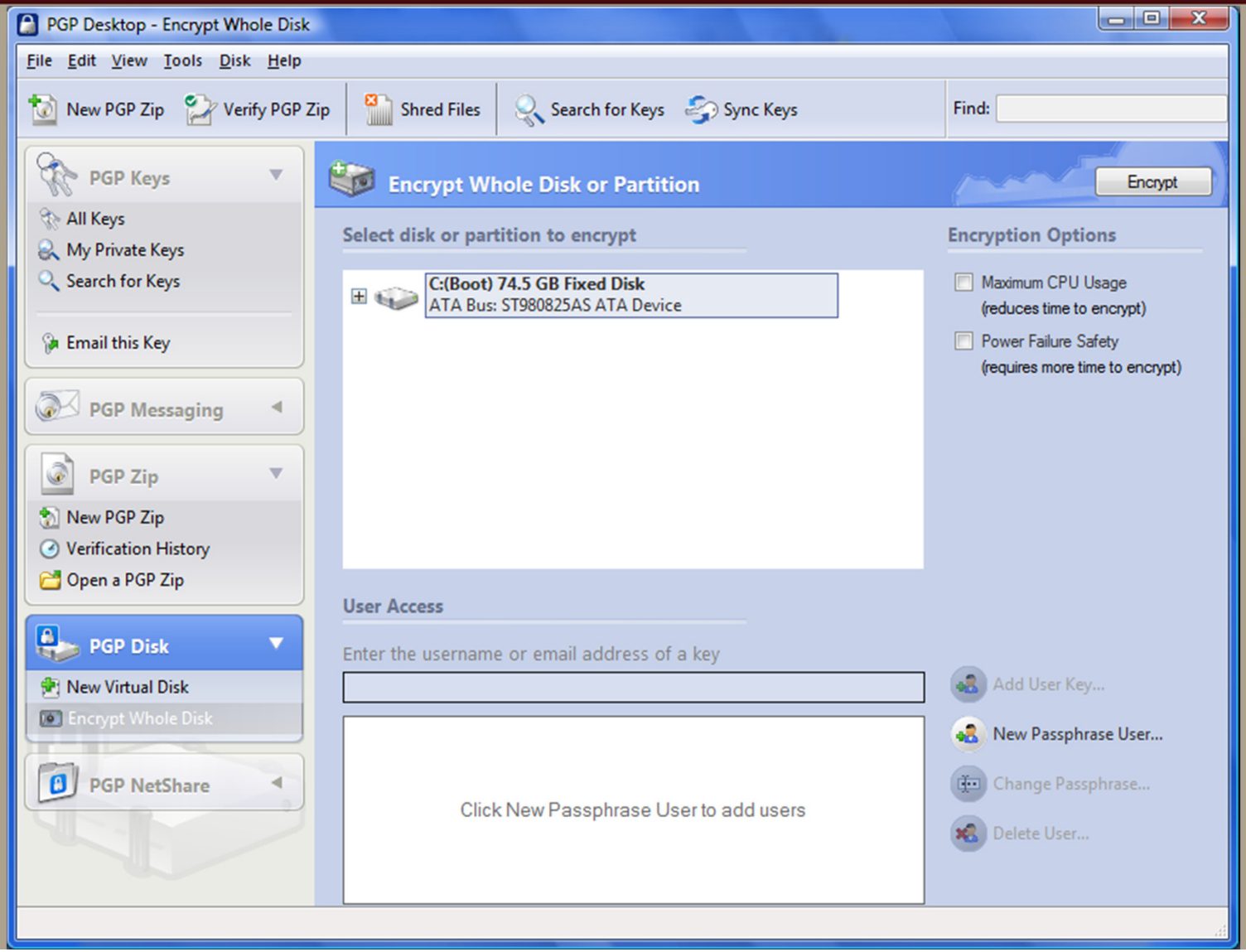
LEHIGH UNIVERSITY

PGP Desktop



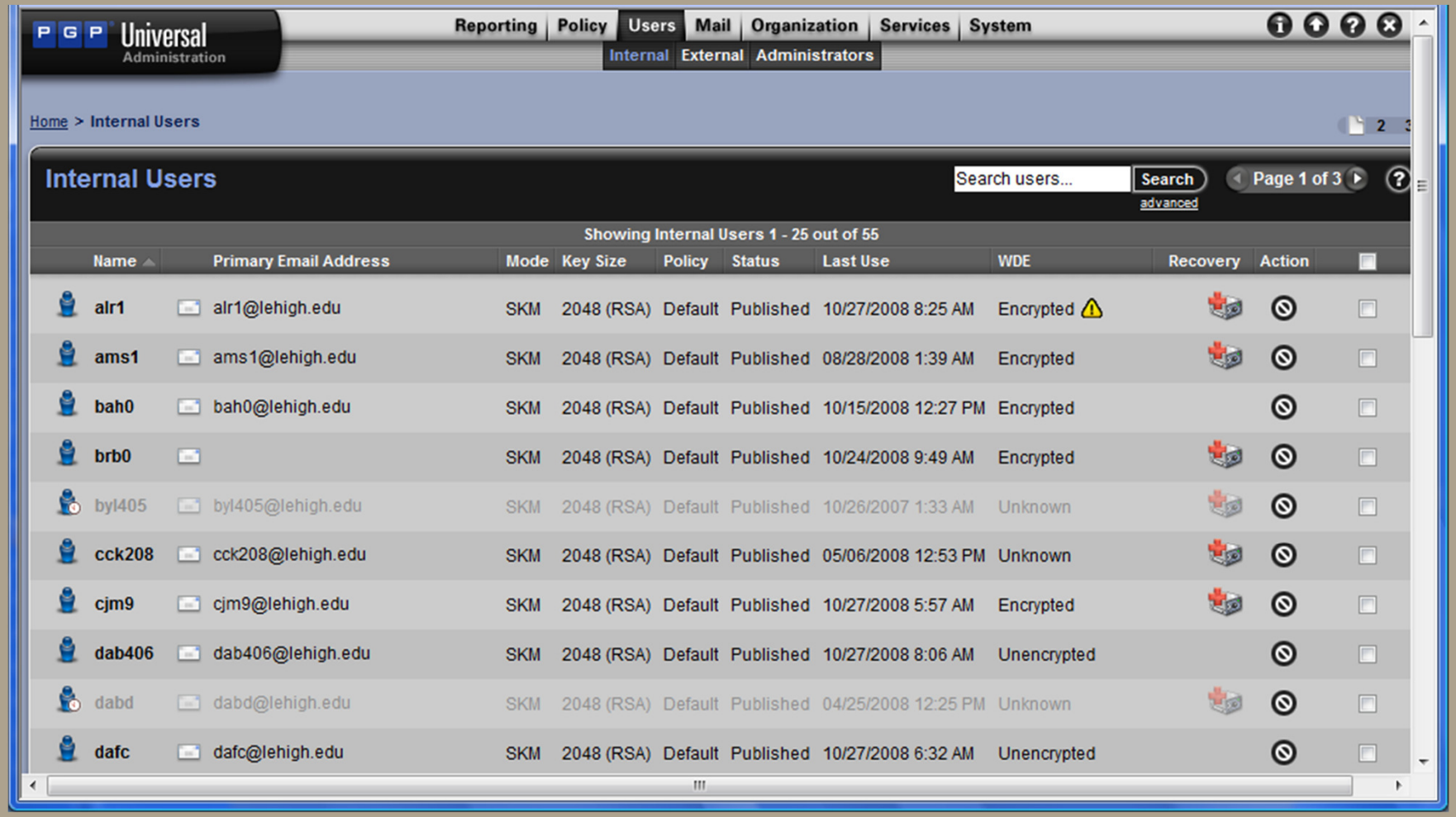
LEHIGH UNIVERSITY

PGP Desktop



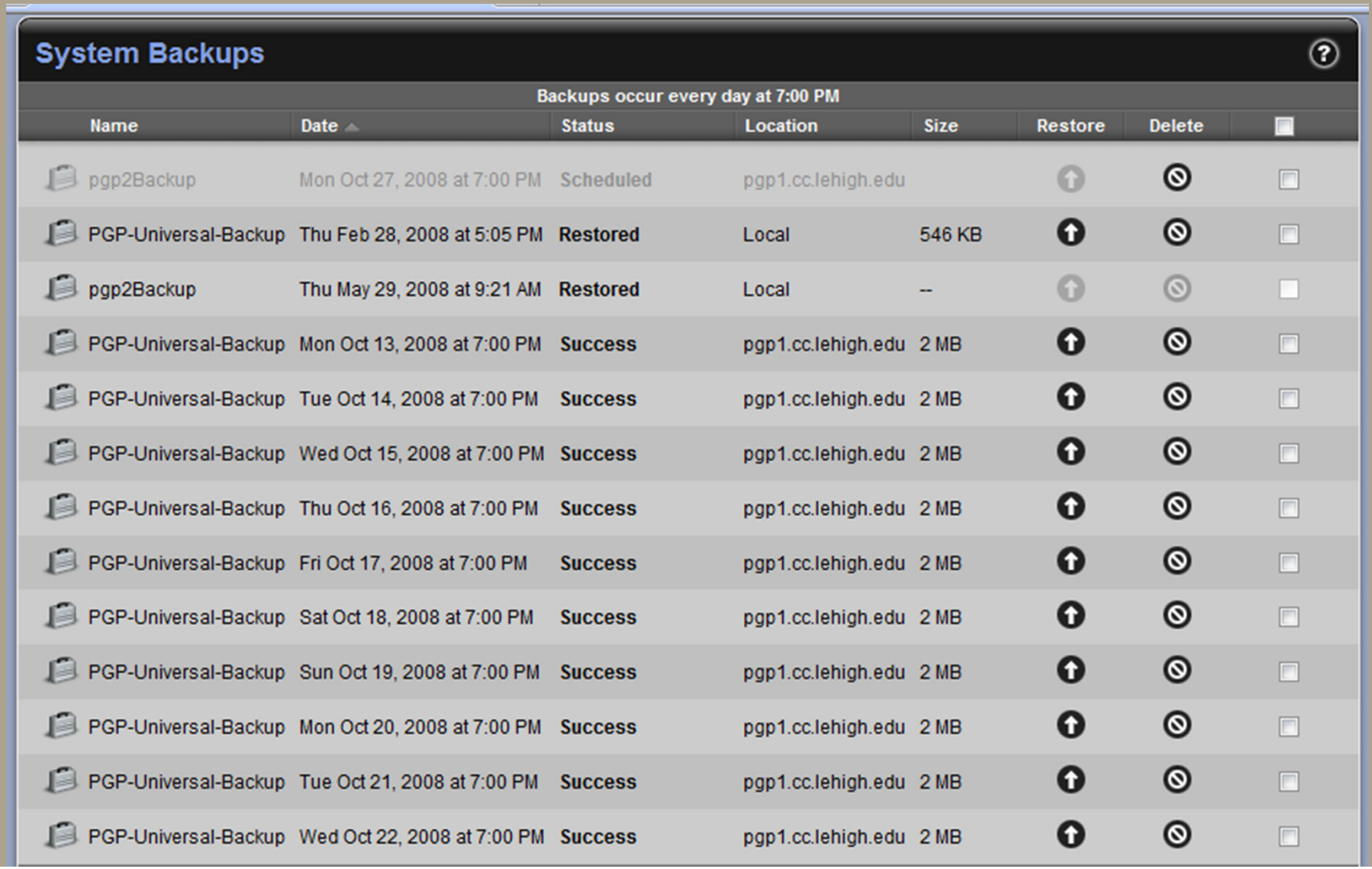
LEHIGH UNIVERSITY

PGP Universal Server



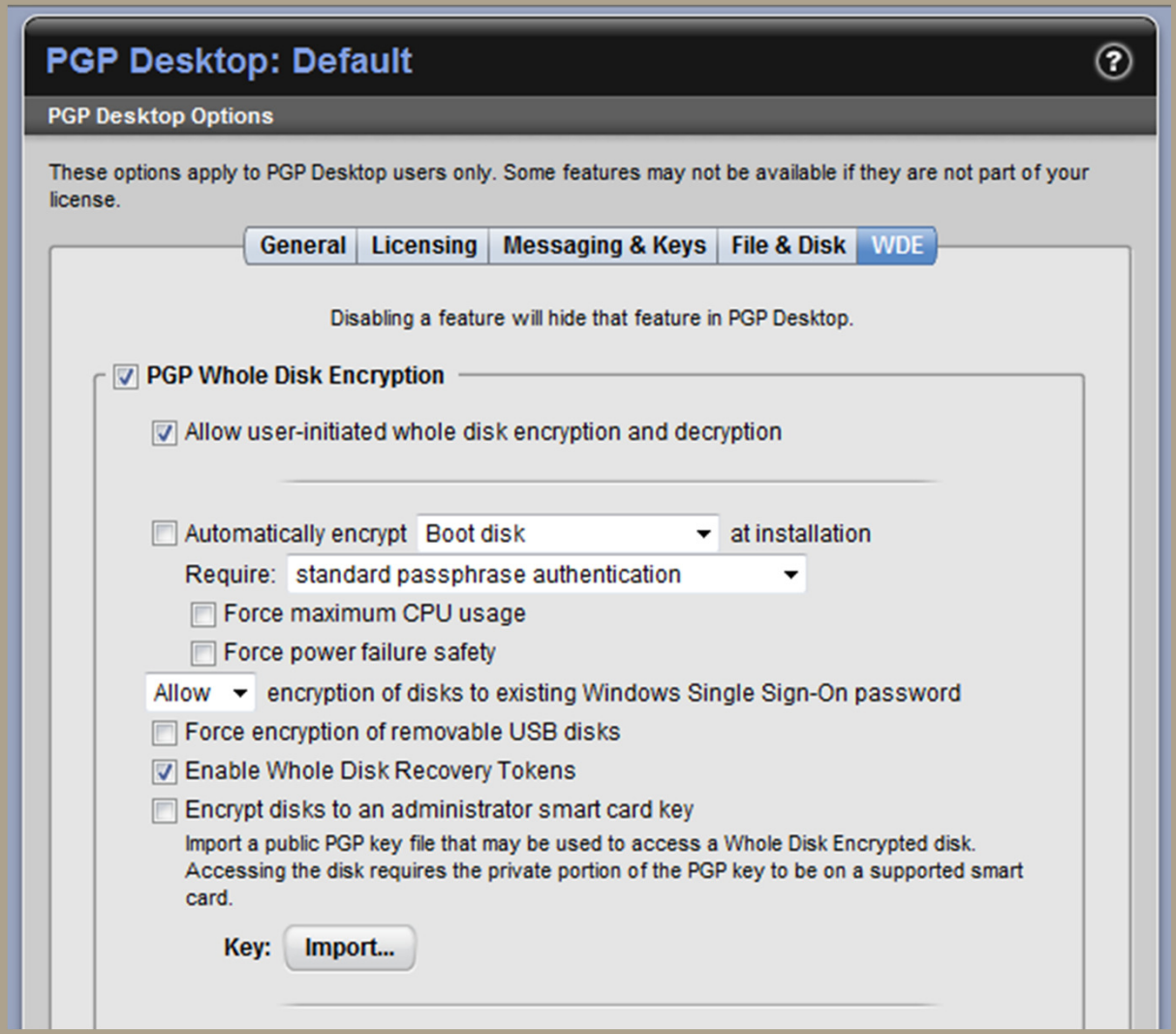
LEHIGH UNIVERSITY

PGP Universal Server



LEHIGH UNIVERSITY

PGP Universal Server



LEHIGH UNIVERSITY

PGP Pilot Program

(October 2007 – May 2008)

- 100 Copies of PGP Desktop and Universal Server
  - Funded by Library and Technology Services
- 3 Groups of individuals were identified as testers
  - Technical Users (first installation)
  - Administrative Users (second installation)
  - Academic Users (third installation)
- Training was scheduled for each test group
- Policies were set and a customized installer created
- Hard drives were purchased to backup user data
- Web-based Feedback form created using Cold Fusion

LEHIGH UNIVERSITY

Pilot Program Results

- PGP was installed on 69 computers (54 users)
- 36 users provided feed back
  - 51% reported no problems
  - 15% reported encryption process took too long
  - 12% reported slowness opening applications
  - 10% reported slowness opening drives
  - 10% reported slowness on boot
  - 2% reported errors while encrypting drive

LEHIGH UNIVERSITY

PGP Pilot Survey

Response Rate: 40%

Questions	Responses		
What type of computer do you have?	Laptop: 36%	Desktop: 64%	
How long have you been a PGP Whole Disk Encryption user?	Less than 3 months: 23%	3 to 6 months: 46%	More than 6 months: 31%
Why did you decide to use the software?	Concern for my use of sensitive data: 46%	My boss told me I had to: 27%	Other: 32%
Who installed your software?	LTS: 64%	Myself: 34%	Other: 0%
Do you perform regular data backups?	Yes: 27%	No: 68%	I Don't know: 5%
If Yes, are your backups encrypted?	Yes: 25%	No: 50%	I Don't Know: 25%
How much of a concern is "Confidence of Recovery of Encrypted Data" if you forget a password or something happens to your computer	A small concern that can be easily managed: 36%	A significant concern that can be managed : 22%	A huge concern that will be difficult to manage: 22%

LEHIGH UNIVERSITY

Proposed Implementation Plan

Encrypt all staff computers on campus

- Install PGP on all mobile users first (~ 400 laptops)
  - Finish installing remaining 31 licenses on university laptops (key areas)
  - Purchase licenses to cover remaining laptops and encrypt as soon as possible
- Bundle the price of a PGP license with the new purchase of each PC
- PGP training for staff
- Timeframe
  - October-December 2008 (remaining licenses)
  - January 2009 – December 2009 mobile users
  - incorporate license with new PC purchase (3 year lifecycle)

LEHIGH UNIVERSITY

Issues and Roadblocks

- User's Time to Encrypt
  - Encryption takes 1-3 hours
- Computing consultant reluctance to install the software
- Computing Consultant time to perform installations
- Client reluctance to install software
- Concern over recovery of data if file corruption occurs
- Development of a reliable client backup solution

LEHIGH UNIVERSITY

Questions we asked ourselves

- What happens if a user forgets his/her password?
- What happens if a user changes his/her password on and off campus?
- How do we handle the installation for campus users?
- How do we handle encrypting external USB devices?
- What happens if a user encrypts a USB device and uses a computer that doesn't have PGP?
- Should we require user files be backed up? If so, how?

LEHIGH UNIVERSITY

Contact Information

Gale Fritsche – gale.fritsche@lehigh.edu

Tim Foley – tim.foley@lehigh.edu