

# ITS Executive Steering Committee (ITESC)

Agenda and Materials  
October 19, 2007



*Preparing people to lead extraordinary lives*

# Agenda

---

1. Credit Card Processing Project Review - Nitha Nagubadi, Kevin Smith (15 minutes)
2. Emergency Notification System - Phil Kosiba (15 minutes)
3. Security Program and Assessment Results - Jim Sibenaller (25 minutes)
4. Data Center Services Status and Planning - Dan Vonder Heide, Wayne Sliwa (30 minutes)



# Agenda

---

1. Credit Card Processing Project Review -  
Nitha Nagubadi, Kevin Smith (15 minutes)
2. Emergency Notification System - Phil  
Kosiba (15 minutes)
3. Security Program and Assessment Results -  
Jim Sibenaller (25 minutes)
4. Data Center Services Status and Planning -  
Dan Vonder Heide, Wayne Sliwa (30  
minutes)



# Marketplace

Agenda:

What is it?

Who is involved and how we progressed?

Formalizing processes and procedures, & documentation

Overview of projects

How to proceed with requests?



# What is it?

- New TouchNet ecommerce software purchased by Finance department.
  - Tool to allow departments to sell products, bill for items, such as parking tickets, or sell registration for events.
  - Very user friendly shopping cart features.
  - Relatively easy to create stores within certain restrictions.
  - 2 different components - Ustore and Upay



# Who is involved and how we progressed?

Who worked on it? – Joint effort between CMS (Cory O'Brien in Treasurer's office) and ITS (Web Team- Cheryl, Pat, and Nitha).

Consulted with Marketing for initial design setup of the mall.

Currently Loyola's first credit card Privacy Policy is being drafted and reviewed by general counsel.

3 phases: Training, Installation/Implementation, Upgrade.

- Training: March 1, March 2
- Installation on production of Version 3: May 17
- Upgrade on test server of Version 4 : June 8
- Upgrade to Version 4 and verification complete on production: July 24
- Released first 2 stores for Conference Services to production: May 22.



# Formalizing processes & documentation:

## General Process:

- After reviewing business plan, CMS decides on approval and priority of the departmental use of online CC processing and submits SSR to ITS.
- ITS in conjunction with PRB reviews the request and prioritizes and initiates it as an official project in PSS.
- ITS and CMS meet with departments to gather detailed business requirements.
- ITS documents and builds ustore and/or upay site.
- CMS and ITS train the users on policies and how to use the store's administrative and reporting features.



# Documentation

## Completed Documentation:

1. General Outline that provides overview of coordination of efforts between CMS and ITS of entire project cycle from initial request to production release.
2. Updated credit card policy on CMS website:  
<http://www.luc.edu/finance/casmgm.shtml>
3. Business Requirements Questionnaire for departments who are using the online credit card processing.
4. Training documentation on reports, issuing refunds/cancellations, store use, and Credit Card Policy.

## In Progress Documentation:

1. Working on creating comprehensive Demo and overview of Marketplace documentation for departments.
2. Working on documentation to provide overview to departments on the overall process and their responsibilities from initial request, training and production.





# Completed Stores

<b>Department</b>	<b>Store</b>	<b>Completion Date</b>
Conference Services	2 Stores- CS Payments, CS Incidentals	May 22
Academic Affairs	Parent's Weekend	August 27
Career Center	Fall Career Fair	September 10
ITS	ITS Training Courses (non credit card)	September 14
School of Education, Catholic Conferences	3rd Annual Conference on Instructional Leadership	August 31



# Stores Approved and In progress

<b>Department</b>	<b>Store</b>	<b>Completion Date</b>
LUMA	Membership	November 1
LUMA	Events	November 1
LUMA	Museum	Will begin review after other 2 stores in production.
SCPS	Dr. Atomic (1 day Symposium)	November 13
Academic Affairs	Discover Loyola	June 2008
SCPS	Continuum – Conversion to Upay	When clients are ready.
Human Resources	Training Courses	November 9
Academic Affairs	Training Courses	November 9
Preschool	Tuition	December 15



# Stores Pending Approval

<b>Department</b>
Theology
Bioethics
Continuing Medical Education
Social Work
Executive Education
SSOM Ministry



# Demos

<b>Department</b>	<b>Date</b>	<b>Outcome</b>
SPCS – Dr. Atomic Event	September 26	Project Started, production date is November 13 <sup>th</sup> .
Executive Education – Registration for Courses	September 26	Interest expressed in Continuum type of site
Alumni and Special Events	October 5	Department not interested; they want the ability to build and maintain their own stores.



# How to submit requests.

- If you have a interest in credit card usage, please start with reviewing the information on
  - Cash Management Website  
<http://www.luc.edu/finance/casmgm.shtml>
- If you would like a demo before a request is made, please contact [webmaster@luc.edu](mailto:webmaster@luc.edu)
  - Demo store:  
[https://epay.luc.edu:8443/C20996test\\_ustores/web/store\\_main.jsp?STOREID=27](https://epay.luc.edu:8443/C20996test_ustores/web/store_main.jsp?STOREID=27)



# Agenda

---

1. Credit Card Processing Project Review -  
Nitha Nagubadi, Kevin Smith (15 minutes)
2. Emergency Notification System - Phil  
Kosiba, Susan Malisch (15 minutes)
3. Security Program and Assessment Results -  
Jim Sibenaller (25 minutes)
4. Data Center Services Status and Planning -  
Dan Vonder Heide, Wayne Sliwa (30  
minutes)



# Emergency Notification System

---

## Initial Prioritization Results:

Pri	Row	Prog	PSS Nbr	Project Description	Prioritized Ranking by Function							Ranking		
					AA	Adv	Fac	Fin	HR	SA	IIS	Score	Rank	
B	74			Emergency Notification (AlertNow etc.)							7		14	54

Reprioritize to “A”; assess impact to other projects

---

Sample Notification System through IIT’s Website:

<http://www.iit.edu/iitalert/>



# Agenda

---

1. Credit Card Processing Project Review -  
Nitha Nagubadi, Kevin Smith (15 minutes)
2. Emergency Notification System - Phil  
Kosiba (15 minutes)
3. **Security Program and Assessment Results -  
Jim Sibenaller (25 minutes)**
4. Data Center Services Status and Planning -  
Dan Vonder Heide, Wayne Sliwa (30  
minutes)





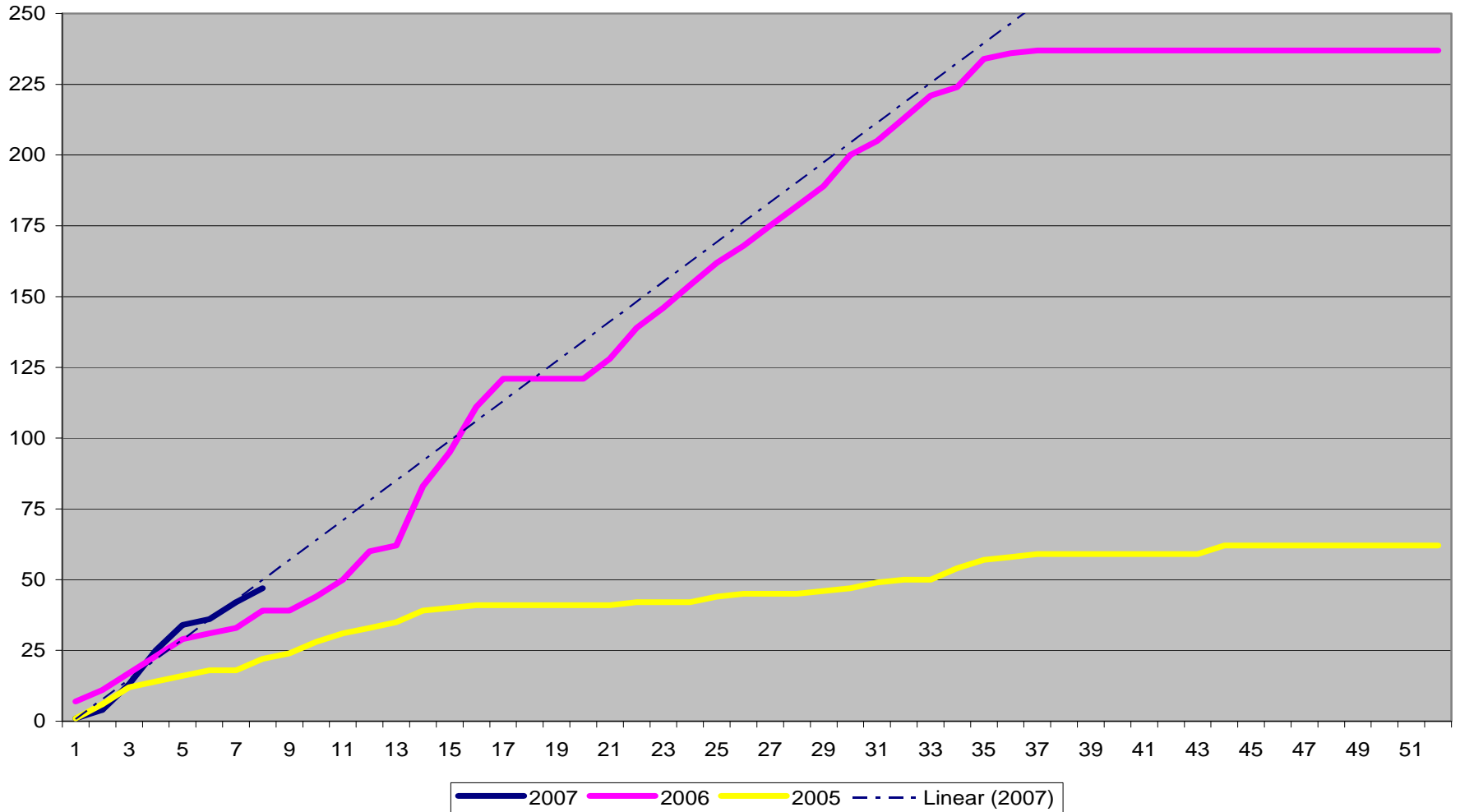
# PIRG Status

---

- Policies
  - Cabinet revisions in progress
  - SAUPC approval received
    - Clarification of relevance to university staff at LUMC
    - Recommendation for a Corporate Compliance Officer at each campus
    - Clarification of “IT Contracts” in place, process etc.
  - FAUPC not available for review until 11/16
- Training materials in final draft
- Awareness materials in progress
- PII identification & disk encryption software being piloted in ITS

# DMCA Status

DMCA Violations - Cumulative Totals



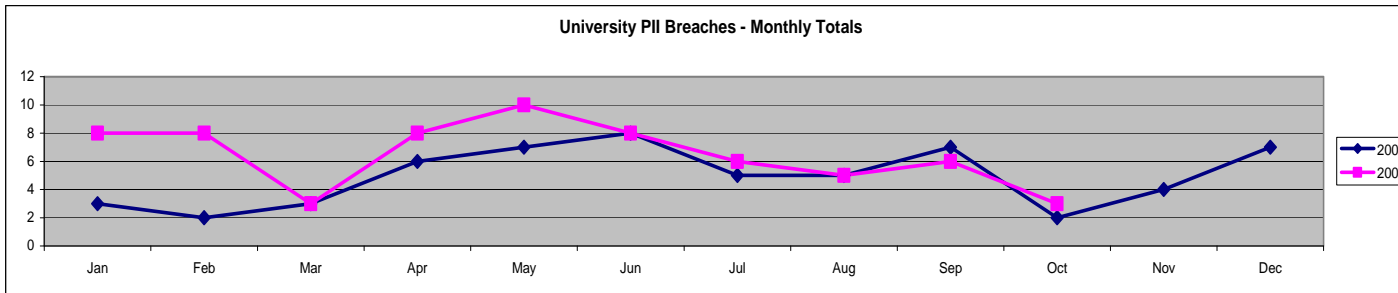
Date	University Count	YTD Counts	University "Highlights"	Other Institutions
Jan 2006	3		Pitt, <b>Notre Dame</b>	H&R Block
Feb 2006	2		Old Dominion	Fed Ex, Ernst & Young
Mar 2006	3		<b>Georgetown</b>	<b>Chicago Olympic Funding</b> , US Marines, Fidelity Investments
Apr 2006	6		<b>Purdue</b> , Texas	Dept of Defense, Mastercard
May 2006	7		Ohio U, Delaware, Miami	Wells Fargo
Jun 2006	8		Miami OH, Kentucky, <b>Western IL</b>	Ernst & Young, IRS, US Navy, ING
Jul 2006	5		<b>USF</b> , Tennessee, <b>Northwestern</b> , Iowa	Sentry Insurance
Aug 2006	5		Kentucky, Wichita State	AFLAC, US Dept of Transportation
Sep 2006	7	46	Virg Comm., Minnesota, Colorado	<b>City of Chicago</b> , Lloyd's of London, General Electric
Oct 2006	2		Texas, Minnesota-Spain	US Census Bureau, T-Mobile, <b>Chicago Voter Database</b>
Nov 2006	4		Virginia, Cal State	Starbucks, American Cancer Society
Dec 2006	7		UCLA, Mississippi State, Emory	Aetna, Boeing
Jan 2007	8		<b>Notre Dame</b> , Arizona, Rutgers, <b>Eastern IL</b>	<b>Chicago Board of Elections</b> , IRS
Feb 2007	8		Missouri, Nebraska, Johns Hopkins	US Dept of Veteran Affairs
Mar 2007	3		Montana, Idaho	Radio Shack, US Dept of Agriculture
Apr 2007	8		UCSF(2), Pitt Med Center, OSU	<b>Chicago Public Schools</b> , TurboTax, CVS Pharmacy, Neiman Marcus
May 2007	10		<b>Northwestern</b> , Colorado, LSU, Missouri	<b>Illinois Dept of Financial Regulation</b> , IBM, J.P. Morgan, Lucent
Jun 2007	8		<b>Northwestern</b> , Iowa, GA Tech, Virginia	Pfizer, American Airlines
Jul 2007	6		Michigan, Texas A&M, <b>Purdue</b>	Pfizer, FOX news, SAIC (Pentagon Contractor), TSA, Disney, <b>Fidelity</b>
Aug 2007	5		<b>Loyola Chicago</b> , Yale, <b>Illinois</b>	AT&T, Monster, Verisign, Merrill Lynch
Sep 2007	6	62	<b>Purdue</b> , Kansas, Michigan, Johns Hopkins	Pfizer, Gander Mtn., Gap Inc., eBay
Oct 2007	3*		Iowa, Carnegie Mellon	Pfizer, Commerce Bank

\* Note - Through 10/13 only

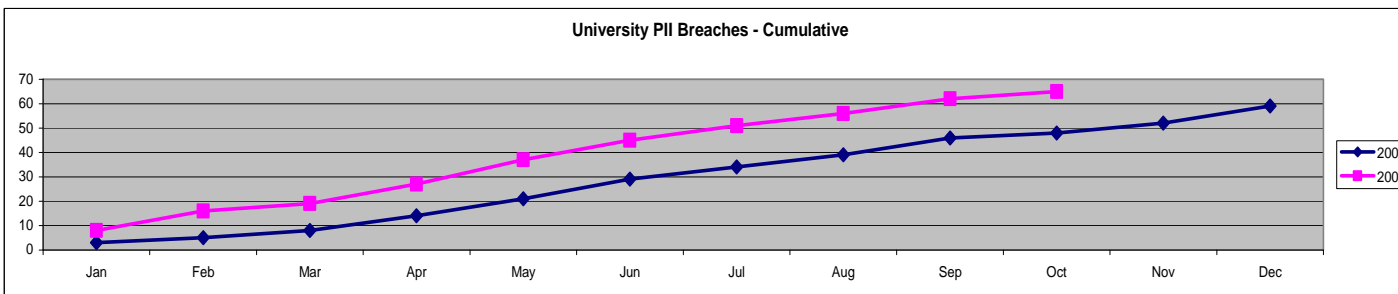
# PII Industry Update

PrivacyRights.org

University PII Breaches - Monthly Totals



University PII Breaches - Cumulative



Preparing people to lead extraordinary lives

# Information Security Concerns - Industry

---

1. Education and Awareness
2. Validating user-supplied input
3. Insecure Communications
4. Data Classification
5. Identity and Access Management
6. Intrusion Detection Systems
7. Viruses, Botnets, Rootkits, Phishing
8. New Attack Vectors (IM, P2P, Flash)
9. Information Leakage/Loss
10. Excessive User Rights

*Sources: Gartner, SANS Institute, PCWorld, IT Management Earthweb, SearchCIO-Tech Target, OWASP.org*



# Information Security Priorities

---

- **Gartner 2007: Higher Education Top 10 CIO Technology Priorities**
  - #1 Security
- **Gartner 2006: Spending Priorities for CIOs**
  - #2 Security technologies
- **Educause 2007: Top 10 CIO Issues to Resolve**
  - #2 Security
- **CIO Magazine 2007: Top 10 IT Concerns**
  - #5 Security
- **Society for Information Management (SIM) 2007: Top 10 IT Management Concerns**
  - #6 Security and privacy



# Information Security Assessments

---

- **2006 SMART LLC**
  - External & Internal Testing
    - Network assessment, Modem Access, Wireless assessment
  - Application Assessment
    - High-level application assessment, Examination of SDLC
  - Results: *“Based on our experience with other Colleges and Universities, Loyola University of Chicago has a **relatively low number of external vulnerabilities, and very few of the more egregious internal vulnerabilities that we typically find at other higher education institutions.**”*
  - Findings: 6 high, 5 med, 3 low
- **2007 Berbee Information Networks Corp/CDW**
  - Web Application Testing
    - 11 applications
  - External “Hardening” Measures
    - Validate changes implemented after last assessment
  - Results: *“In the course of the review, the Network Security Engineer’s were impressed with a number of aspects of the Loyola environment...”* and *“...Loyola has **much stronger security practices as compared to other universities** they have examined.”*
  - Findings: 16 high, 13 med, 5 low



# Information Security Risks - Berbee

---

## 2007 Key Assessment Findings - Berbee

1. Improve input edits and validation
  - SQL injection
  - LDAP injection
  - XSS attacks
2. Change System Admin password on Palladium (badge access). Advised to validate physical server locations.
3. Work with Campus Card and Blackboard to improve security on the Blackboard Transaction Server.
4. Regular auditing of system and database passwords.
5. Move away from clear-text protocols for authentication.
6. Password protect Oracle listener ports.
7. Bring in instructor to provide secure coding training.



# Information Security Risk Response

---

- Personal Information Risk Group (PIRG)
  - PII Protection
- Assessments
  - FY06 - SMART & Assoc.
  - FY07 - Berbee
  - FY08 - If budget allows
  - FY09 - Ongoing request
- FY08 Security Admin Position
  - Hiring process active
  - Expanded capacity & support
  - Improved monitoring & metrics
- Information Security Program





# Information Security Program












---

## Program Highlights

- Identified **128** items of concern
- Categorized & Mapped
  - *Applications*
  - *Network*
  - *Audit*
  - *Passwords*
  - *Awareness*
  - *PII Data*
  - *Database*
  - *Policies*
  - *Desktop*
  - *Servers*
- Risk levels defined
- Efforts analyzed & timings planned



# Information Security Scorecard

<u>Technology/ Operation</u>	<u>Unhealthy</u>		<u>Healthy</u>
Applications	No secure coding training available, secure coding practices not used uniformly, user input not checked for validity.		Secure coding training available, secure coding practices used by developers, user input checked for validity.
Audit	No formal security audits are performed.		Annual security audits are performed in reference to passwords and physical access.
Awareness	End users not educated about and not automatically protected from threats. Training not available.		End users informed and automatically protected from threats. Security training available for all staff and required.
Database	Databases and associated services not secured according to best practices, such as inappropriate passwords, irregular patching, and non-protected services.		Databases and associated services secured according to best practices, including appropriate passwords, regular patching, and protected services.
Desktop	Non-unique passwords shared between desktops, users able to install software, and no backup tools available to users.		Desktops appropriately secured, including passwords and software install limitations, appropriate backup tools for users.
Network	Standard network security tools not present or not monitored by ITS staff.		Standard network security tools are in place and routinely monitored by ITS staff.
Passwords	No password standards published, no automated checks to check password complexity.		All passwords adhere to published standards, automated systems confirm that new passwords adhere to standards.
Personally Identifiable Information (PII) Data	PII usage and storage location is not known, controlled or measured. Compliance unknown.		PII usage and storage location known and data properly protected. Monitored for compliance.
Policies	Policies and guidelines not identified for all common information security issues.		Policies and guidelines published for all common information security issues.
Servers	Servers maintained outside of data center, not configured securely, not routinely patched, logs not regularly monitored.		Servers maintained in ITS data center, securely configured, routinely patched, logs regularly monitored.

# Agenda

---

1. Credit Card Processing Project Review - Nitha Nagubadi, Kevin Smith (15 minutes)
2. Emergency Notification System - Phil Kosiba (15 minutes)
3. Security Program and Assessment Results - Jim Sibenaller (25 minutes)
4. **Data Center Services Status and Planning - Dan Vonder Heide, Wayne Sliwa (30 minutes)**

