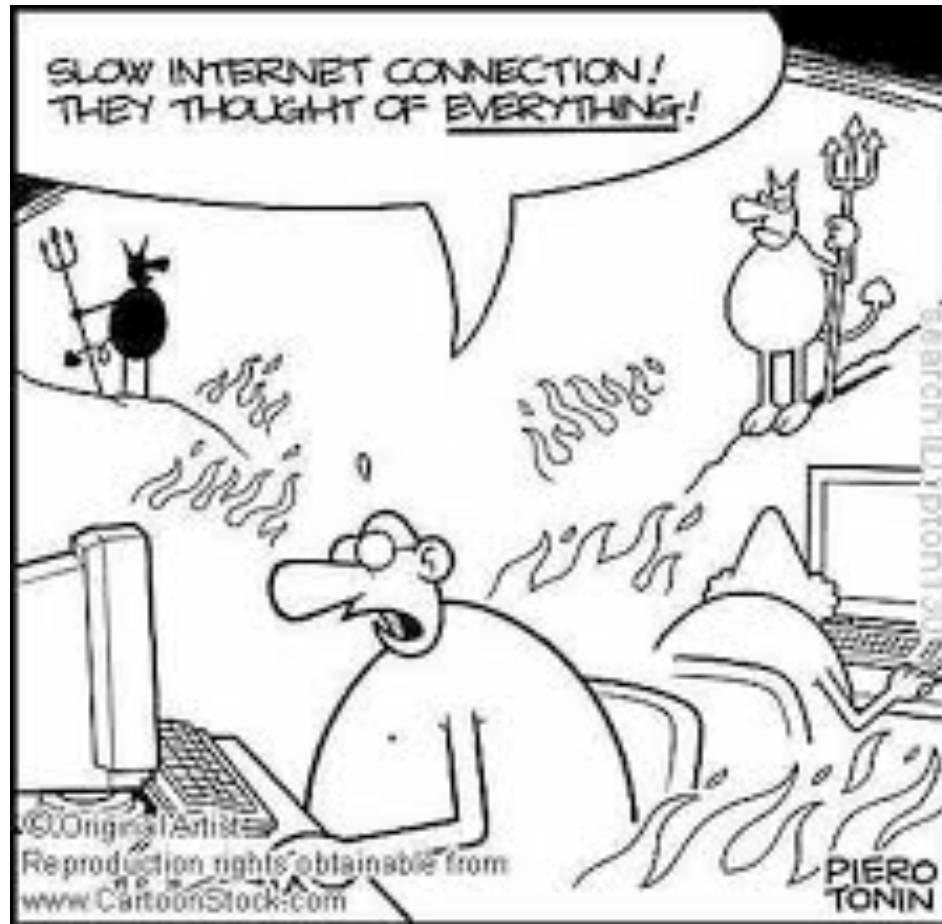# IT Briefing

1/20/11

Agenda

- Exchange 2010 Update
- Eagle Mail Update
- Service-now Update
- SMCC Update
- Symantec Upgrade
- Shibboleth Update
- Security Update
- PCI Project Awareness

- Jay Flanagan
- Jay Flanagan
- John Wilson
- Luciano Dalla Venezia
- Tom Armour
- Elliot Kendall
- Brad Judy
- Brad Judy & Graydon Kirk
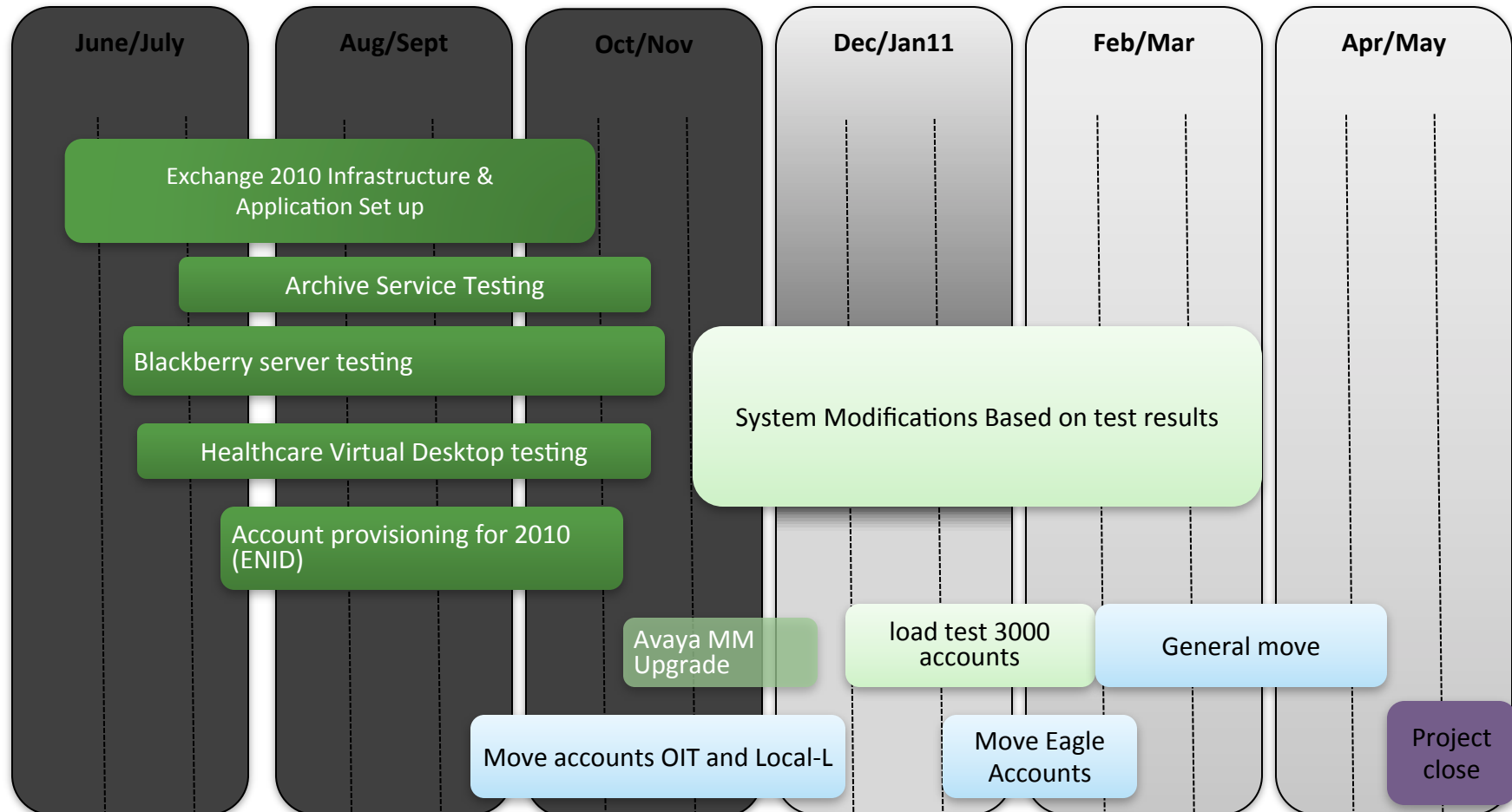
Exchange 2010 Project

Jay Flanagan

Exchange 2010

Monthly Updates

– Over 1200+ accounts on 2010

  • Local Support

  • College

  • Nursing

  • Pathology

– In February:

  • GBS

  • Oxford

  • SPH

Exchange 2010

Open Issues

- Archiving
  - EAS OWA – Close
    - Search issue fixed
    - Another issue was exposed
  - Unstubbing in 2010
    - Continuing to work with the vendor
- Eagle Migrations/Moves
  - First test accounts complete
- Creation of new Exchange accounts on 2010
  - Work is in process and will begin soon at a date to be determined

Exchange 2010

High level schedule - January

June/July	Aug/Sept	Oct/Nov	Dec/Jan11	Feb/Mar	Apr/May

Exchange 2010 Infrastructure & Application Set up

Archive Service Testing

Blackberry server testing

Healthcare Virtual Desktop testing

Account provisioning for 2010 (ENID)

System Modifications Based on test results

Avaya MM Upgrade

load test 3000 accounts

General move

Move accounts OIT and Local-L

Move Eagle Accounts

Project close

7

Eagle Decommission Project

Jay Flanagan

Eagle is going away!

Eagle Decommission

Latest Info:

- 5600 accounts still to move off of Eagle Mail
- Continue to work with schools and departments to move accounts
- The Exchange Team has set up specific servers for the purpose of moving Eagle users to Exchange 2010
  - Completed this past week
  - Currently running initial tests
  - After initial testing the first groups to move will be the College and Pathology

Eagle Decommission

The Process

- Migrate Eagle users to the Exchange 2007 Special Servers
- Work with Local Support to make sure all user data was migrated
  - This step is important as once the user is moved to Exchange 2010, any data not migrated from Eagle will need to be moved to Exchange 2010 manually
- Move users to Exchange 2010
- Archiving is not a factor while users are on 2007; they will be archived when moved to 2010

Questions

Update – *Select Highlights*

Making Progress…

- – Resolved/Closed 144 SN incidents since 11/5/2010
- – As of 12/19 – 9 Incidents remain

MIN page redesign

Old page

Major Incident Notifications

ACTIVE ALERTS

Service List Date Incident Number Short Description Last Update

RECENTLY CLOSED ALERTS

Service List	Date	Incident Number	Short Description	Last Update
	2011-01-19 10:54:00	INC764313	MIN -Control-M abend null null	

Service-now

EMORY UNIVERSITY | **University Technology Services**

New MIN page (it.emory.edu/status)

Major Incident Notifications

ACTIVE ALERTS »

Service(s) Impacted	Date	Incident	Description
IT Service Management	2010-12-28 10:23 AM	INC522536	Testing MIN's again on DEV, part deux **Priority: 4 - Low** **Impact Details »** Features Unavailable: Printing Locations Affected: My computer Users Affected: Me **Latest Update »** 2010-12-28 10:34 AM Checking print function
Room and Space Management	2010-12-28 09:42 AM	INC522534	Testing MIN updates in Dev1 **Priority: 5 - Planning** **Impact Details »** **Latest Update »**
Digital Media Gallery	2010-12-19 04:50 AM	INC519479	MIN- Luna insight digital media gallery is currently unavailable **Priority: 3 - Moderate** **Impact Details »** **Latest Update »**
IPS	2010-12-15 12:32 PM	INC476459	FYI - Decommission of the old Intrusion Prevention (IPS) units that are monitoring the ResNet links. **Priority: 1 - Critical** **Impact Details »** **Latest Update »**
IT Service Management	2010-11-01 01:10 PM	INC019040	FYI - IT Service Management

Service-now

- ## System Performance
  - Issue to be resolved in Winter 2011 release (February)

- ## Service-now Outage – 1/14 (INC717395, INT1873905)
  - Down for about 40 minutes
  - 18% of SN customers affected
  - Root Cause – duplicate IP address on SN proxy server
  - Silver Lining: Communication with the vendor was very good

- ## What's next?
  - SLA rewrite
  - Prioritized backlog
  - Additional training - reporting

Questions

SMCC Update

Year in review

- SMCC was formed around 1 year ago
- Modules that have gone live in Service-now:
    - Change Management
    - Knowledge Management
    - Incident Management

- Time to renew membership

SMCC Update

Steering Body Members

- Mark Conde, School of Public Health
- Chuck Elliott, School of Medicine
- John Ellis, UTS
- Carole Meyers, Emory College
- Ginger Kane, DAR

SMCC Update

SMCC Members

- Amir Ali, UTS
- Sharon Gregory, UTS
- José Rodriguez, UTS
- Tiffany Kady, School of Public Health
- Danon Vaughn, DAR
- Laura Pokalsky, Emory College
- Joel Thomas, School of Medicine

SMCC Update

Non-voting SMCC Members

Represented by the UTS IT Service Management Office and the Service-now Service owner

- Enid Britton, UTS-ITSMO
- Farah Remtulla, UTS-ITSMO
- Luciano Dalla Venezia, UTS-ITSMO
- John Wilson, UTS-Business Systems

Questions

smcc@emory.edu

Symantec Endpoint Protection 11

Tom Armour

Migration History

SEP 11 Upgrade

Server Updates

- Jul 2009 - initial install SEP11 mr4mp2

- Oct 2009 - update to SEP11 ru5

- Apr 2010 - update to SEP11 ru6a

- Oct 2010 - update to SEP11 ru6mp1

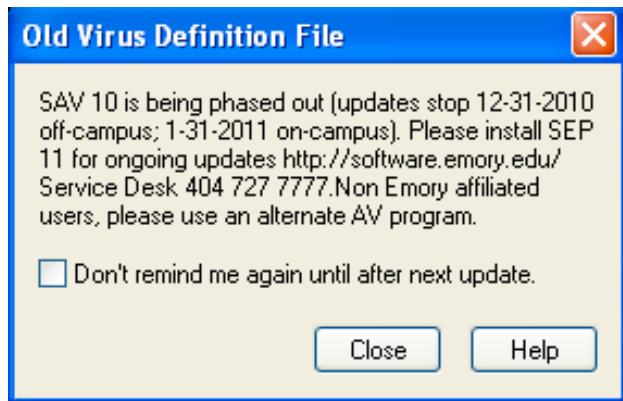# SEP 11 Upgrade

Symantec AntiVirus 10 Status

- Retiring Symantec Antivirus 10 Server (Wolf-vm)

- Our goal, communicated in February, was to have everyone off this server by Aug 31, 2010

- Dec 30, 2010 - turned off all external Internet access to SAV 10 (Wolf-vm) (DONE)

- Jan 31, 2011 - turning off for internal use

Communication

- DeskNet
- IT Briefing
- Local-L
- Application Notification: (What we Wanted)
  - Your virus definitions are currently out of date. Emory is phasing out Symantec Antivirus 10. Please remove this software and install Symantec Endpoint Protection 11 for ongoing updates (http://it.emory.edu/catalog/virus_management/). You may contact the OIT Service Desk at 404.727.7777 or your departmental Local Support on how to update them.
  - If you are no longer affiliated with Emory, please find an alternate antivirus program like Microsoft Security Essentials.

Communication

- Technical issue with software

  - SAV can only display 5 lines of 50 characters each, so we had to re-work the message

- Application Notice (Actually used)

  - SAV 10 is being phased out (updates stop 12-31-2010 off-campus; 1-31-2011 on-campus). Please install SEP 11 for ongoing updates http:/ software.emory.edu/ Service Desk 404 727 7777.Non Emory affiliated users, please use an alternate AV program.

Questions

Emory Login
AKA Shibboleth

Elliot Kendall

Emory Login (Shibboleth)

- Web single sign-on
- Strong OIT support for wide adoption
- Federated sign-on across institutions
- Easy to use – UTS will provide simple instructions
- Delegated access control
- A single shared login page for all apps
- De-facto higher ed standard
- Free and open source

The story so far

Current Emory Login apps

- UTS Web Hosting (includes many other apps)
- OIT Wiki
- Emory Blogs

The story so far

Coming soon

- Cayuse
- Service-now
- Gartner access
- Software Express
- Mysoft Shopping Cart
- Educause
- Internet2 wiki
- [your app here]

How do I get it?

UTS Web Hosting

- Built-in support! Very easy to use

- Usual method with .htaccess

- Can limit access to certain NetIDs, or all Emory users

- For more details, search Knowledge Base (it.emory.edu/kb) for "Password protecting"

How do I get it?

Non UTS hosted

- Install some software on your server (Apache or IIS – Java and others possible but trickier)

- Fill out some forms

- Email us

- We configure some things on our end

- For more details, search Knowledge Base (it.emory.edu/kb) for "Shibboleth"

How do I get it?

Vendor-hosted apps

- Ask if vendor supports Shibboleth or SAML
- If so, have the vendor contact webgroup@emory.edu

Outstanding issues

Single sign-out

- Not currently supported – "close your browser"

- May be in a limited form in future

- For high-security apps, can require re-authentication

A new standard

UTS recommends Emory Login

- We recommend using whenever possible
- Direct LDAP connections discouraged
- Plan new apps accordingly
- Consider refitting old apps

Questions

Security Update

Brad Judy

45

What is PCI?
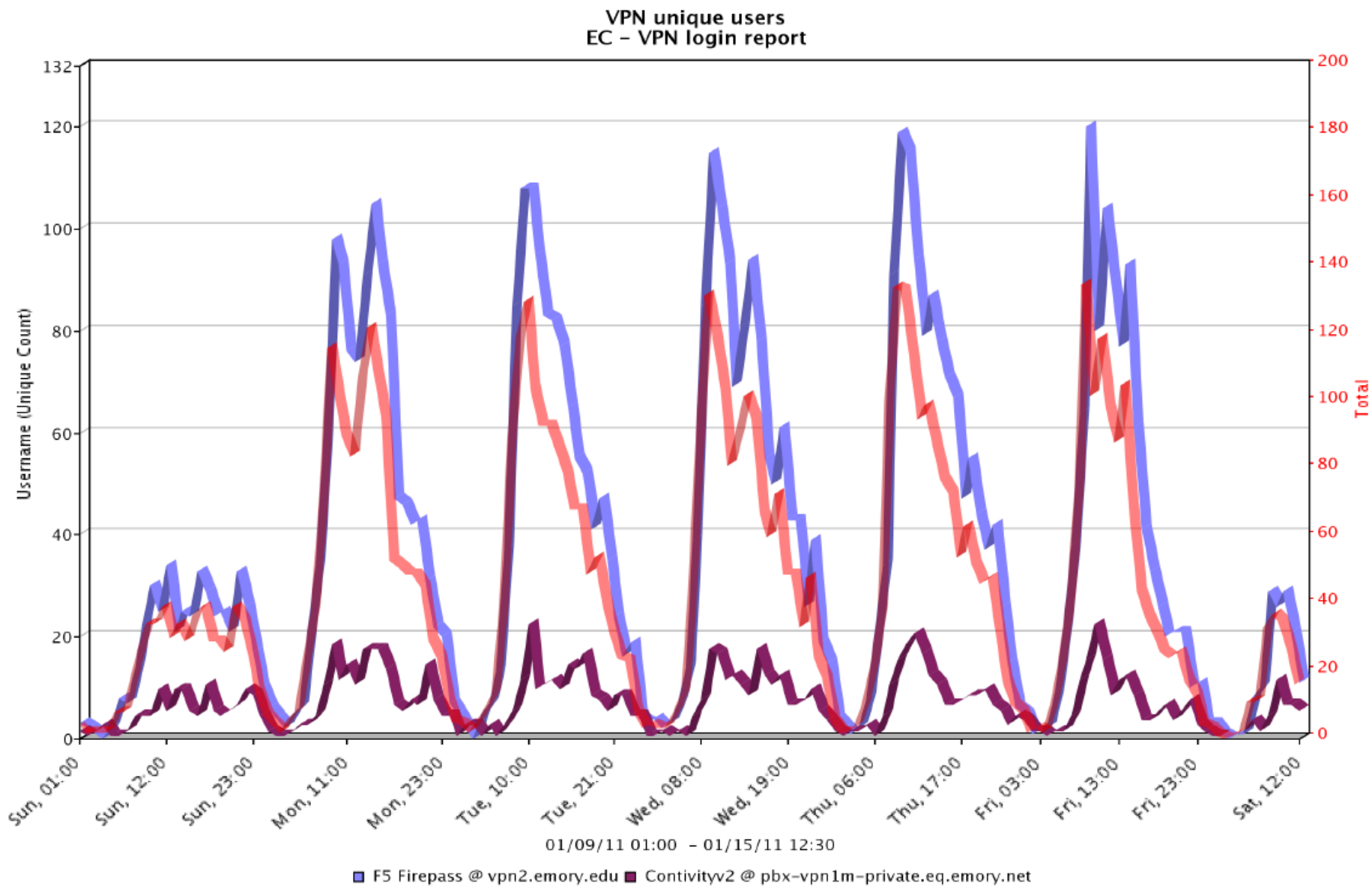
PCI = Payment Card Industry

Think: Payment Card Data Security

The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

https://www.pcisecuritystandards.org/security_standards/index.php

47

ASV's
&
QSA's

Service
Providers

Card
Brands

PCI Council

Acquiring Banks

Merchants

- PCI-DSS
  - Six categories with twelve sections
  - 200+ total items (only 26 apply to swipe-and-dial only merchants)

- Applies to all merchants and service providers, regardless of size

- All merchants must annually self-assess compliance or hire a third-party assessor

PCI requirements

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Project W's

- <u>What?</u>   A project to assess our payment card practices and provide a roadmap to reach PCI DSS compliance and identify a vendor to do periodic security scans

- <u>Why?</u> Ensure compliance and provide for future security scans

- <u>When?</u> Anticipated completion timeline, ~4/30/11

- <u>Who?</u> Division of Finance, OIT Information Security, UTS PMO, EHC/TEC Finance & Information Services

Project Scope Inclusions

- Obtain senior management's formal organizational assignment of authority and responsibility for a PCI Compliance Program Enterprise-wide

- Identify and engage a PCI DSS Qualified Security Assessor (QSA) to Perform an Emory-wide (University and Healthcare) assessment of payment card processing operations of:
  - high risk computerized and outsourced credit card operations; and,
  - organizational knowledge and acceptance of PCI requirements; and,
  - current credit card processing policies, procedures and flows of debit and credit card transactions; and,
  - adherence to current PCI DSS compliance requirements by processing environments in order to;
  - produce a Gap Analysis and a Remediation Plan (for non-compliant environments).

- Identify and engage a PCI DSS Approved Scanning vendor (ASV) to perform periodic security scans to ensure on-going PCI compliance

Project Scope Exclusions

- Formal Report on Compliance.

- Penetration testing of networked systems.

- Social engineering testing.

- Evaluation of "swipe and dial" only merchants.

Project Comunications

- Business Officers' Forum Briefings – Jan 5th (more as needed)

- Division of Finance – Informational Emails

    – (Policies, Procedures, Organizational Decisions, etc.)

- Project Team - Targeted Merchant Contacts for Internal Assessments, Vendor Assessments, etc.

Project Contacts

If you have questions about the *External PCI Assessment* project, please contact:

- Finance:
  - Michael Schiavoni @ mschiav@emory.edu
  - Kim Pate @ kimberly.pate@emory.edu

- OIT Information Security:
  - Brad Judy @ bjudy@emory.edu

- UTS PMO:
  - Graydon Kirk @ gkirk@emory.edu

Questions

Thank you for coming!