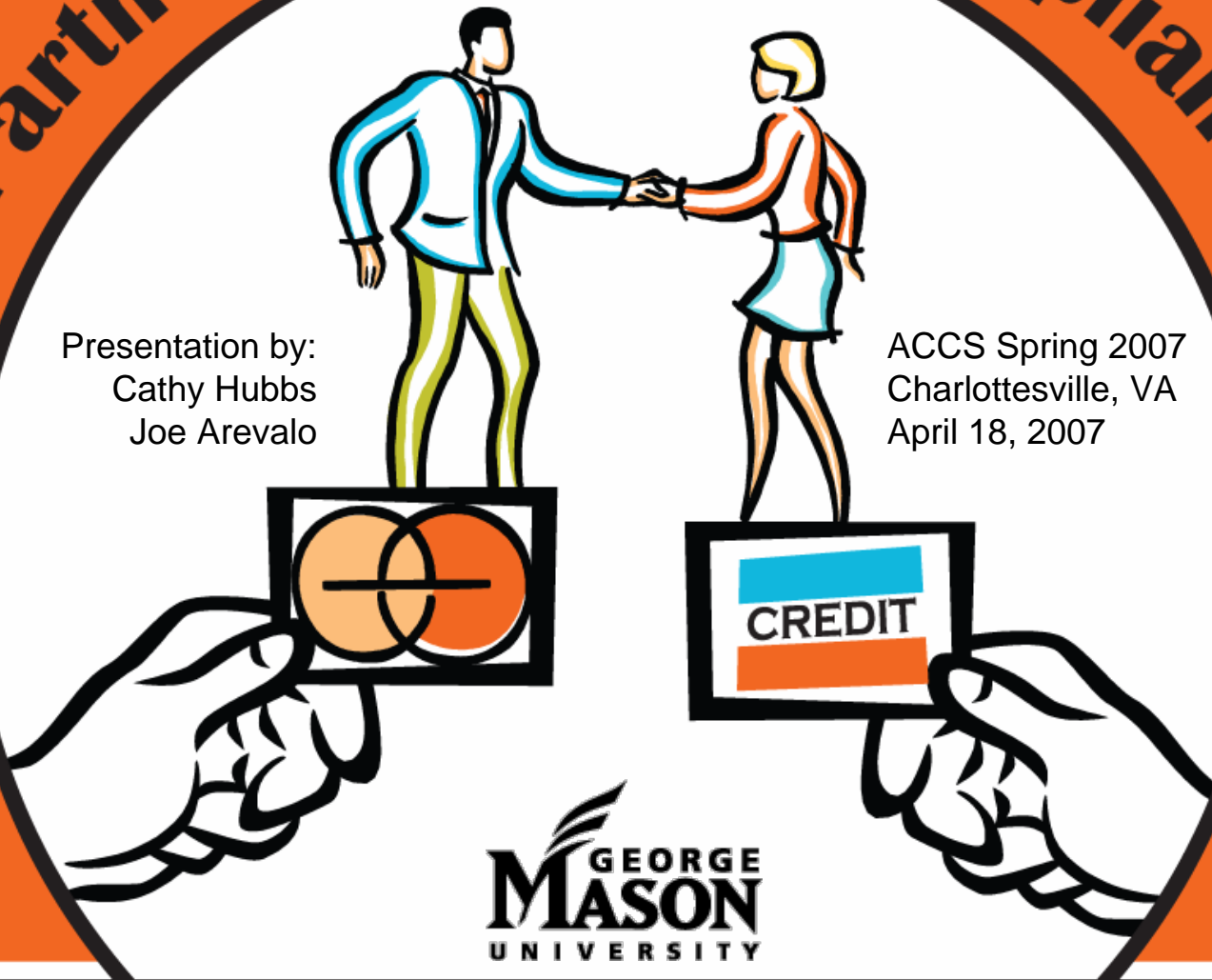


# Partnering for PCI Compliance

Presentation by:  
Cathy Hubbs  
Joe Arevalo

ACCS Spring 2007  
Charlottesville, VA  
April 18, 2007



The logo for George Mason University, featuring a stylized leaf above the text 'GEORGE MASON UNIVERSITY'.

# Today's Talk



- About Mason
- Payment Card Industry (PCI) Primer
- Mason Partners
- Getting Our House in Order
- Segmenting the Network
- Policy & Procedures
- Vigilance

# About Mason



- Public University in Northern VA
- 7,000 staff and faculty
- 30,000+ students, 2<sup>nd</sup> largest in VA
- Four campuses in four counties and UAE
- Most diverse (Princeton Review, 2005)

# PCI Primer



Major credit card companies organized to write a standard for IT Security compliance. In essence the standard states that if an enterprise *stores, processes, or transmits* credit card information they must be compliant. Compliance covers technology used, people, and processes.

# Mason PCI Partners



- Fiscal Services
- IT Security
- Network Engineers
- Systems Engineers
- Internal Audit
- Legal Affairs

# Getting Our House in Order



- What level Merchant are we?
- Defining the scope: who processes CCs?
- Who are the point of contacts?
- Assessing the technology configurations
- Is the processing off campus or campus?
- Is the software compliant?
- Does the University have a policy?

# What are our responsibilities?



- Merchant Level 4
- PCI Requirements
- Questionnaire
- Validated Payment Applications (software compliance)
- Qualified Security Assessor

# Policy & Procedures



- Existing Policy
- New Credit Card Policy
- New Procedures
- Additional places to catch CC processing
  - Help Desk Software (jack activation)
  - Server Registration (assigning IPs)

# Segmenting the Network



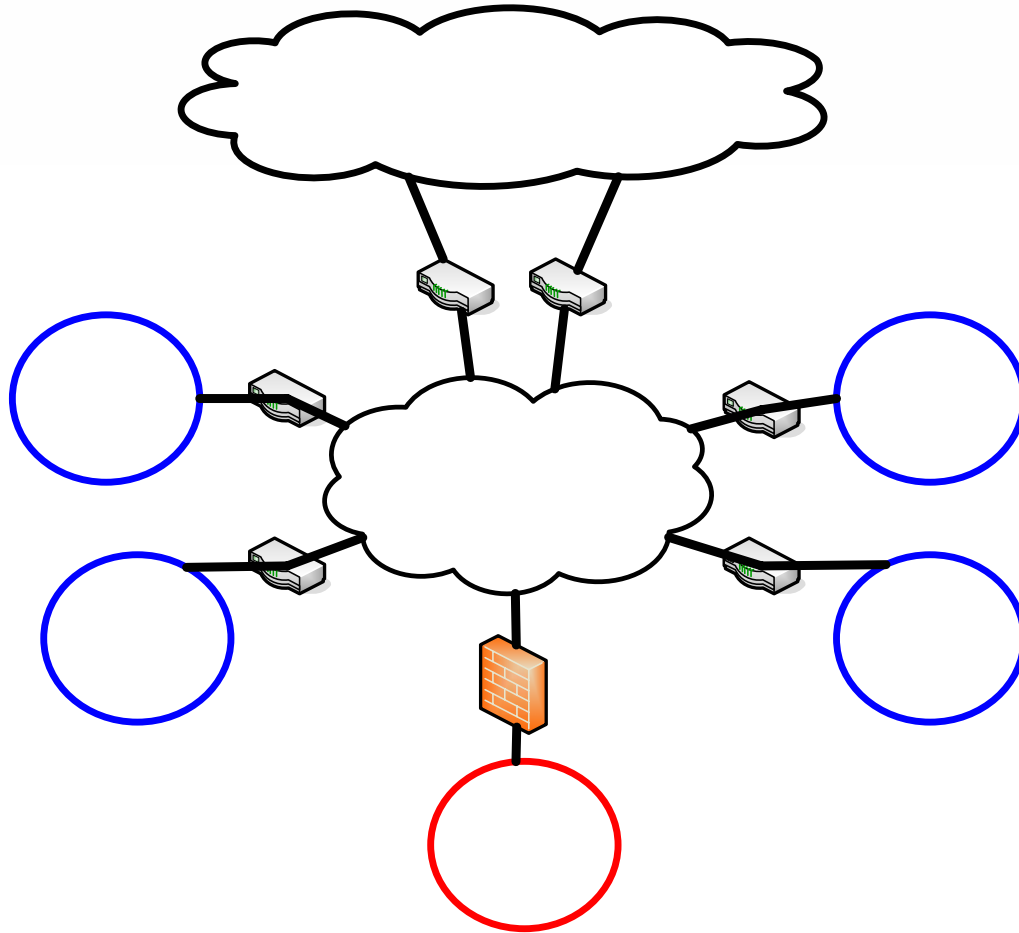
- Assessing the technology configurations
- Who is processing off campus vs. on campus?
- Design & Implementation
- Network Diagrams

# Assessment Info Gathering



- Identify systems and owners
- Gather requirements
- Document topology and data flow
- Assess current measures
- Recommend compensating controls

# Dedicated POS VLANs



# Outsourcing CC Processing



Donate - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.gmu.edu/development/contribute.html

Getting Started Latest Headlines

## ROOT FOR MASON!

## GIVE TO MASON!

Thank you for supporting George Mason University

**Make a Gift**  
Click here to make a secure credit card gift online.

**Make a Pledge**  
Click here to establish a pledge for a single year or multiple years.

**Mail a Card**  
Mail your card or credit card provided by...

**Make a Payment**  
Click here to make a secure credit card payment on an existing pledge.

One Please contact us at [development@gmu.edu](mailto:development@gmu.edu) or (703) 993-8850

Gift Form Pledge Form Payment

Mail to: George Mason Foundation, 4400 University Blvd, Fairfax, VA

Faculty Staff payroll deduction.

Donate - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://www.gmufoundation.org/fndtapps/contribute/donate.cfm?type=credit

Getting Started Latest Headlines

## Give Online

## GEORGE MASON UNIVERSITY

Thank you for supporting George Mason University!

If you have any questions, please contact us at [development@gmu.edu](mailto:development@gmu.edu) or (703) 993-8850.  
Fields marked with \* are required.

**Name and Affiliation**

Title \* First Name \* Initial Last Name \* Suffix

Alumna/Alumnus  Parent  Faculty/Staff  Friend  Student

If alumna/alumnus, Degree Year School Name used at graduation

**Address**

Address Line 1 \*  
Address Line 2  
City \* State \* Zip Code \*  
Country \*  
USA  
Home Phone Work Phone  
Email \* (necessary to receive your confirmation)

**Donation Allocation**

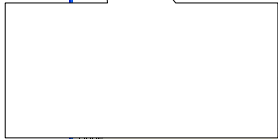
Amount	Purpose
	University Excellence
	General Scholarship
	School Scholarship Fund

--Select School--

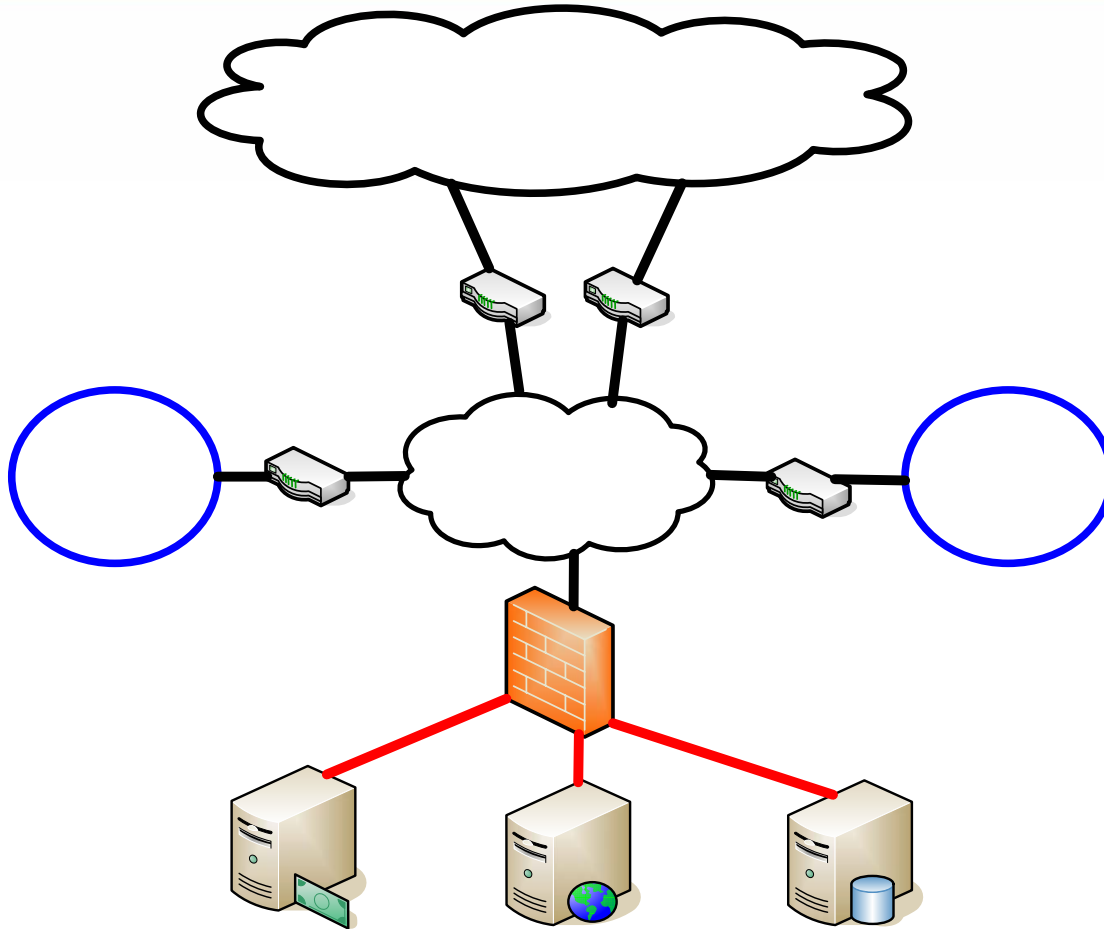
**Recognition Levels**

**President's Circle**

- Senior Benefactor \$100,000+
- Benefactor \$50,000 to \$99,999
- Patron \$25,000 to \$49,999
- Sponsor \$10,000 to \$24,999
- Colleague \$5,000 to \$9,999
- Associate \$2,500 to \$4,999
- Member \$1,000 to \$2,499
- GOLD Circle Graduates of the Last Decade \$500 to \$999

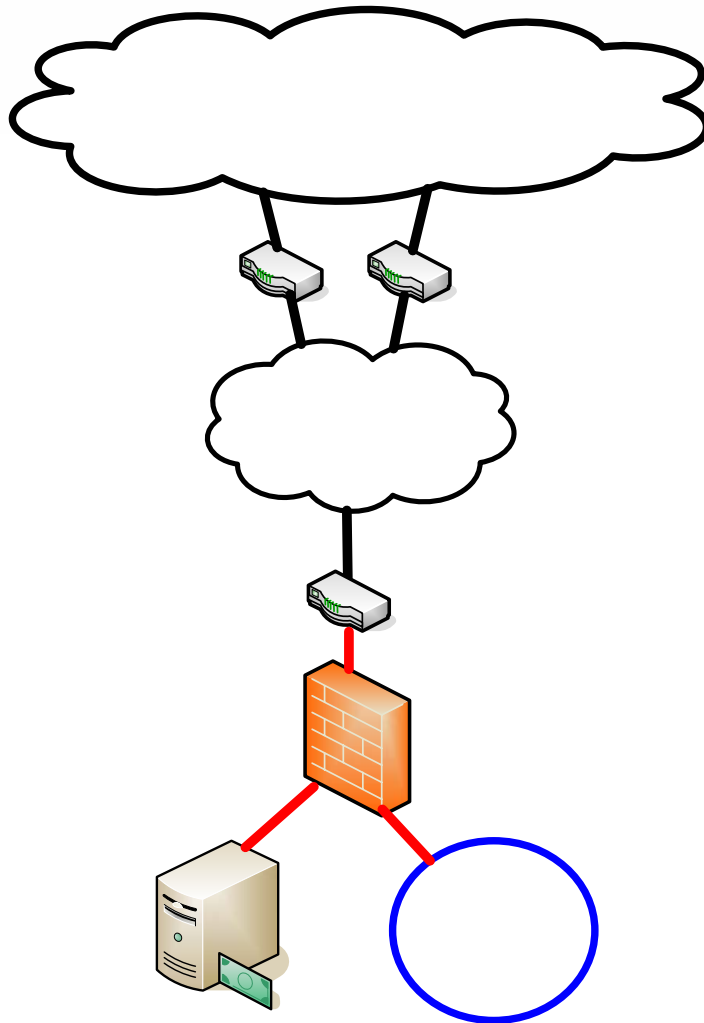


# Centralized



- Servers managed and maintained by Central IT staff.
- Physically located in Data Center server farm.

# Departmental



- Servers managed by individual department.
- Firewall/UTM is installed to provide NAT.

# Vigilance



- Qualified Security Assessor
  - Quarterly scanning
  - Assistance with Questionnaire
- Internal Scanning Assessments
- FW change request
- Distributed FW (UTM)
- Log Management
- Continued dialog and communication with:
  - Fiscal Services (new requests)
  - Central IT
  - Departments new systems, new software applications

# Our Advice



- Define the scope. Get your house in order.
- Gain administration support and participation.
- Identify responsible person to facilitate the PCI process (ongoing).
- Partner for compliance with Fiscal Services and Central IT (at least).

# Comments



Cathy Hubbs, CISSP, CISA

Director, IT Security

chubbs@gmu.edu

<http://security.gmu.edu/>

Joe Arevalo

Network Security Engineer

jareval2@gmu.edu

<http://tsd.gmu.edu/net>

VISA's Cardholder Information Security Program website

[http://usa.visa.com/merchants/risk\\_management/cisp.html](http://usa.visa.com/merchants/risk_management/cisp.html)

