



Massachusetts Institute of Technology
Treasury Institute – PCI Workshop
**Implementing PCI in an Open Network
Environment**
May 5, 2008



Solutions

PCI DSS

CISP

Small Business Compliance

Scanner

ry/start menu/programs/spyarse.../links

Hide details

ned
id

- 0 Processes identified
- 0 Registry keys identified
- 21 Registry values identified
- 28 Files identified
- 5 Folders identified

| Threat Level | Characteristics | Object |
|----------------------|------------------------------|--|
| Potentially Unwanted | View Details | c:\program files\viewpoint\Viewpoint Exp |
| Potentially Unwanted | View Details | c:\program files\viewpoint\Viewpoint Exp |
| Potentially Unwanted | View Details | c:\program files\viewpoint\Viewpoint Exp |
| Potentially Unwanted | View Details | c:\program files\viewpoint\Viewpoint Exp |
| Potentially Unwanted | View Details | c:\program files\viewpoint\Viewpoint Exp |
| Potentially Unwanted | View Details | c:\program files\viewpoint\Viewpoint Exp |
| Potentially Unwanted | View Details | c:\program files\viewpoint\Viewpoint Exp |
| Potentially Unwanted | View Details | c:\program files\viewpoint\Viewpoint Exp |

Abort Scan

Protecting Against 79072 Definitions. Last Definition Update: 2006/07/13 DB-193.

POWERED BY **pareto** LOGIC

Copyright © 2006 ParetoLogic, Inc. All rights reserved.

Agenda

- Situation at MIT when the Project Started
- Project Prioritization, Objectives, Overview
- Payment Gateways
- PCI Compliance Goals, Before and After
- Project Funding, Organization Models
- Conversion Plan
- Solutions Implemented
- Credit Card processing Website
- Project Tools - Communication Plan, Project Statistics
- Lessons Learned
- Situation at MIT Today

MIT Situation When the Project Started (May 2007)

- Over the last 12 months, \$28M in revenue, 200K transactions
- PCI validation is an ongoing process
- Current MIT merchants use a variety of service providers
- Policies and procedures are incomplete and outdated
- Lack of an integrated incident response plan
- Lack of internal MIT process to ensure compliance

MIT Situation When the Project Started (continued)

- 128 MIT Merchants
 - ⦿ 94 Use OMARS/ClearCommerce (onsite payment gateway)
 - ⦿ 20 Use ShopSite (multiple versions – shopping cart)
 - ⦿ 50 web forms (all collecting credit card information)
 - ⦿ 18 Analog Terminals (card present)
 - ⦿ 14 Other Application Solutions (3rd party application, PCI Compliance Certification unknown)
 - ⦿ Merchant developers were all over campus (students, IT, external contractors)

MIT Priority 1 Merchants*

- Priority 1 merchants are MIT's highest dollar and transaction volume merchants, we can summarize their characteristics as:
 - ⊗ **Using a variety of service providers/payment gateways**
 - ⊗ **Increasing their electronic business**
 - ⊗ **Storing and not shredding credit card data on paper/forms**
 - ⊗ **Using onsite servers (MIT assets)**
 - ⊗ **Processing credit cards on shared desktops in open unsecured areas within office suites**

Project Objectives – Business Case

(Phase 1- Assessment, May-September 2007)

- Evaluate:
 - ◆ current state of compliance at MIT
 - ◆ current state of risk at MIT based on merchant procedures and system security
 - ◆ cost and scope of attaining and maintaining PCI compliance
 - ◆ front end service providers, payment gateways and hosting solutions to manage and operate our merchant services
- To provide a high level implementation plan outlining the chosen option (business/system)
- To develop an interim set of policies and procedures prior to selecting and implementing a final vendor

Project Overview - Assessment

- Educate MIT Merchants on the PCI compliance
- Learn about the MIT merchant business
- Identify areas of risk that are uncovered during the data gathering of merchant information
- Evaluate and develop a cost comparison on vendor solutions
- Define cost model for implementation and on-going support of a PCI solution
- Gather information from other higher education institutes on their merchant programs, systems and policies and procedures

Payment Gateways - Moving Target

| Vendor | Status / Reasoning |
|------------------|--|
| TouchNet | Specialize in University Cashiering and Tuition Payments |
| Infinet | Focus is smaller, single merchants, no merchant hierarchy |
| Verisign/PayFlow | No longer a payment gateway, Payflow was sold to PayPal |
| PayPal | Focus is smaller, single merchants, no merchant hierarchy |
| Authorize.net | Sold to Cybersource |
| Google Checkout | Released on 6/28/07, focus is smaller, single merchants, no merchant hierarchy |
| ClearCommerce | No hosted payment page |
| YourPay | Higher Cost, Lack of References, Lack of Professional Services |
| CyberSource | Lower Cost, Many References, Professional Service Capabilities |

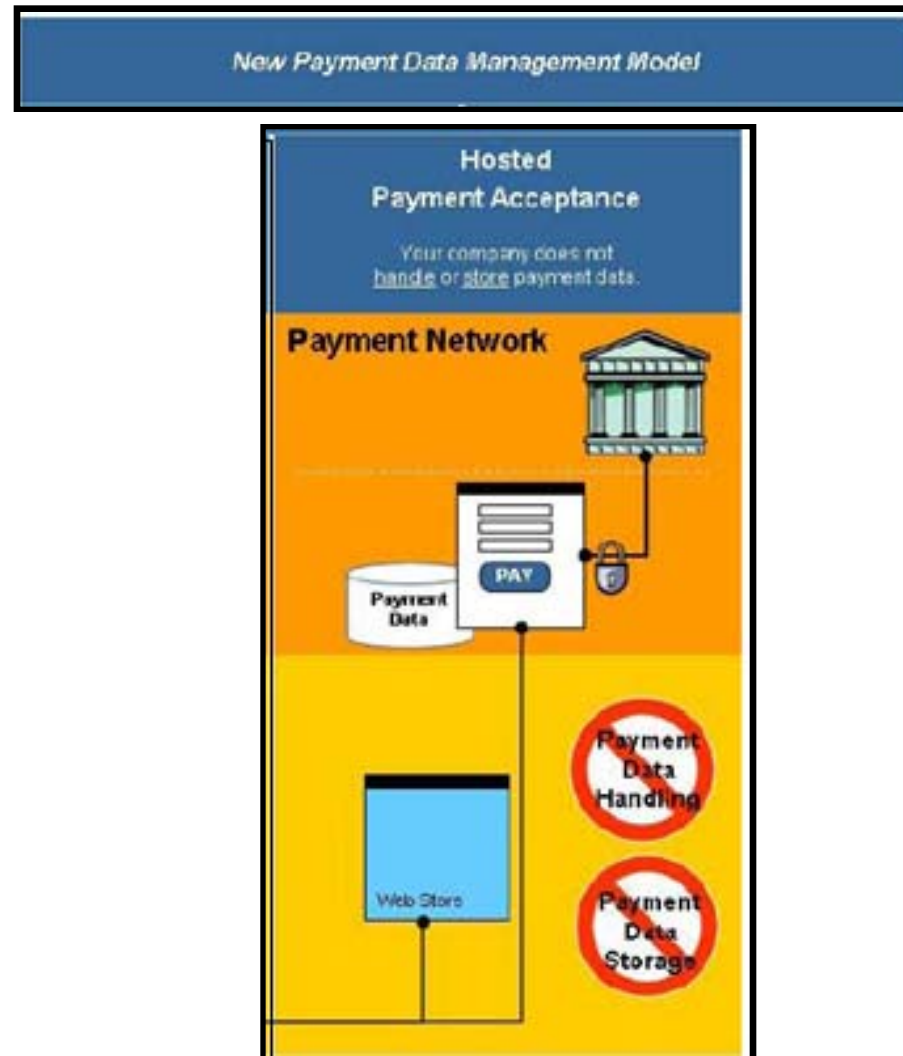
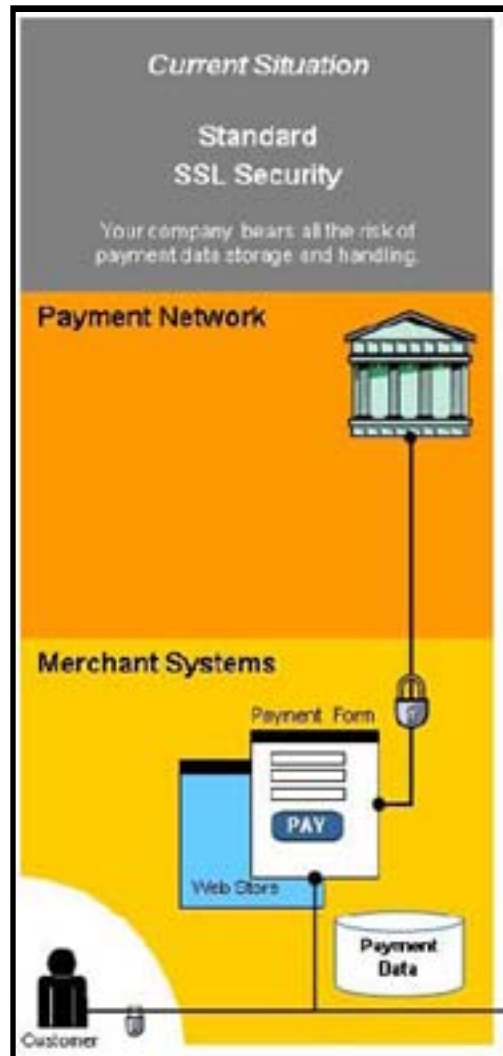
Payment Gateways Evaluated

| | ClearCommerce (Weighted Score) | CyberSource (Weighted Score) | LinkPoint YOURPAY (FDC) (Weighted Score) |
|----------------------------------|--------------------------------------|------------------------------------|--|
| Gateway Features | | | |
| Professional Services Offered | | | |
| Shopping Cart Integration | | | |
| Costs | | | |
| Higher Ed References | | | |
| Non Higher Ed References | | | |

MIT PCI Compliance Project Goals

- MIT's goal to ensure any merchant at MIT that accepts credit cards as a means of doing business will comply with any and all validation requirements as set by the PCI Security Standard Council and the Acquiring Bank This means....
 - ◆ There will be NO credit cards stored on campus anywhere in any format (this means servers, PCs, file drawers, spreadsheets)
 - ◆ All merchants will shift away from credit cards collected via paper form to an automated solution (hosted order page or HOP)
 - ◆ There will be an annual audit of all merchants with self-assessment questionnaires and 3rd party scans of equipment

MIT Before and After



Project Funding

● Resource Plan

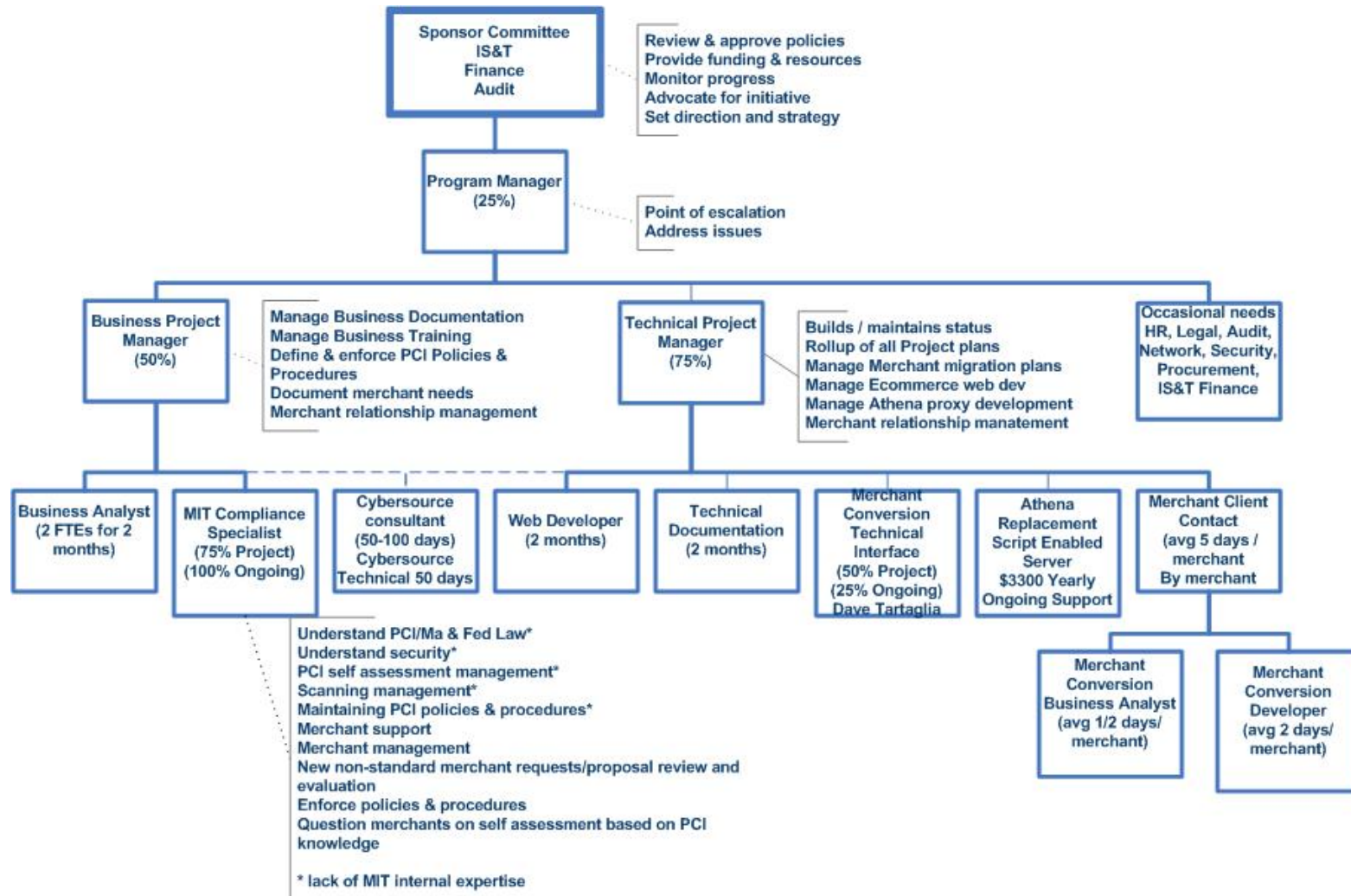
- The costs of the resourcing plan for the Assessment and Implementation Projects were funded centrally through the Controllers Office and IT.

● Merchant Conversion to Hosted Solution

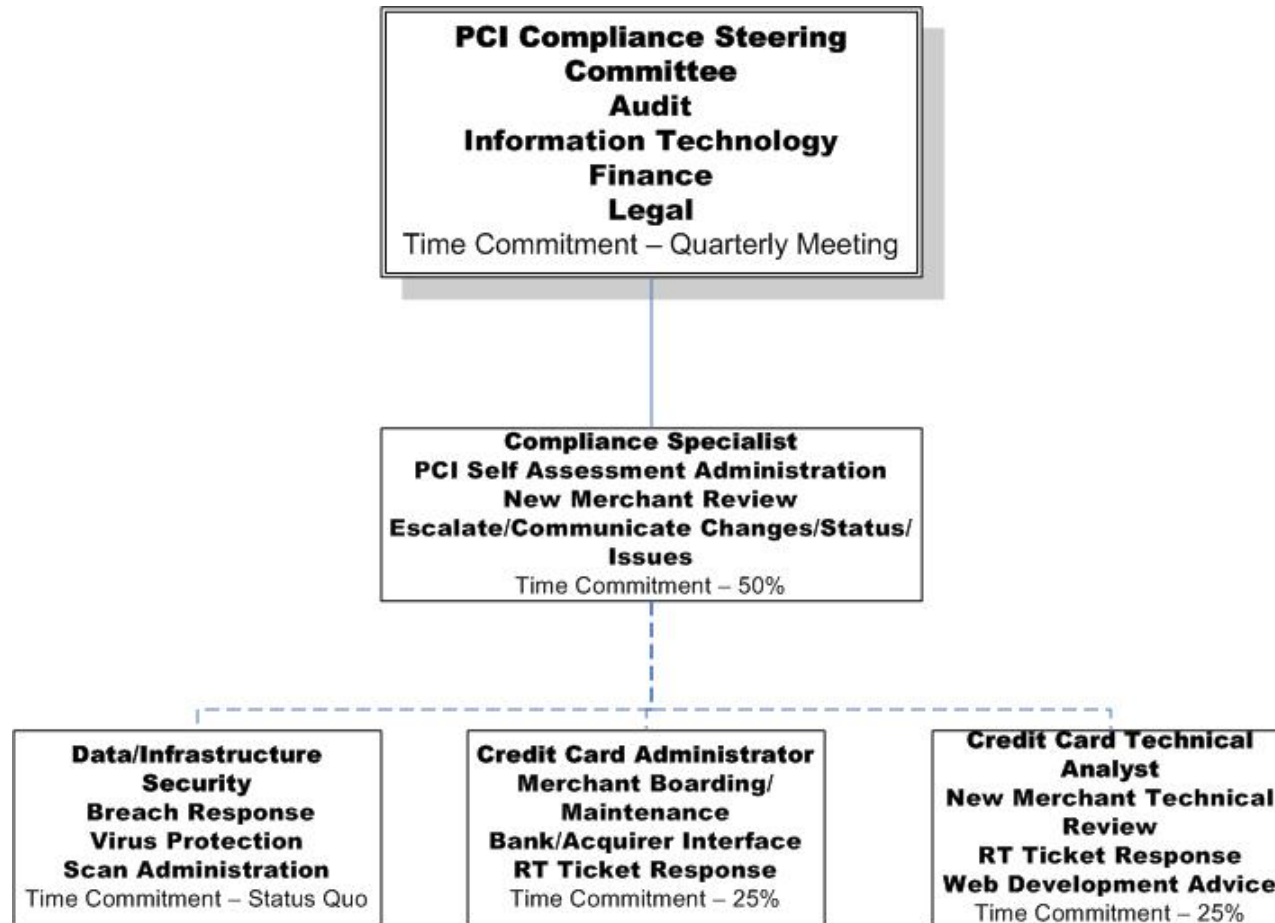
- The cost of converting each merchant was also funded centrally. We allowed \$3500 per merchant for the conversion. The conversion costs were made up of web development, upgraded hardware and developing a web page to eliminate paper processing by merchants.

Note: Most of these allocated costs were not used during the project since the internal team developed a standard web page that was adopted by the majority of merchants.

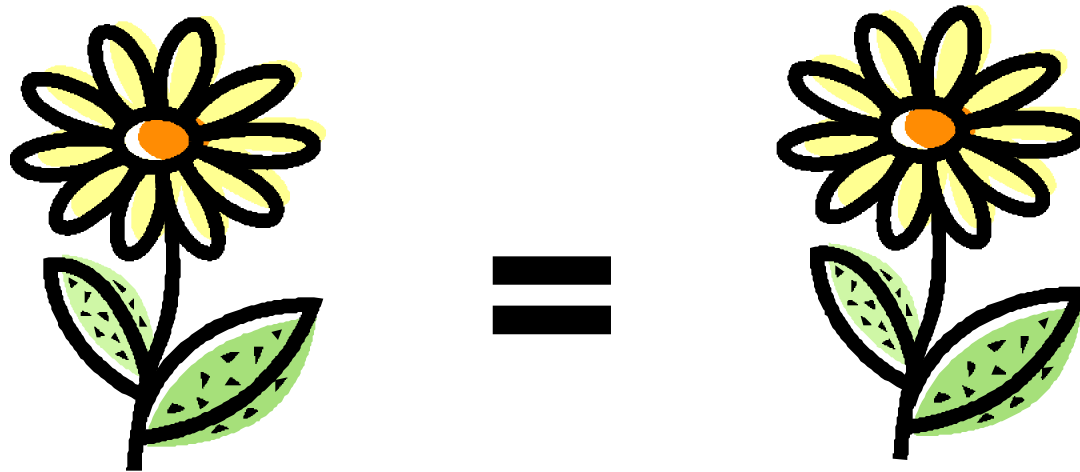
Implementation Organization Model



Ongoing Support Organizational Model



Conversion Scope Creep



- Project team will provide direct assistance in planning migration and actual cutover from your existing Omars/Clear Commerce solution to a Cybersource Solution
- Project team will provide direct assistance in helping custom applications link to the Cybersource hosted order page
- Project team will provide some development support to modify paper back-office function to self service where applicable
- This help will be a same to same, possibly more depending upon your migration
- There will be no new "want to haves" for merchants under conversion - this would be done outside the scope of the project, not covered in the project cost, and cannot impact overall compliance deadline

Solutions Implemented at MIT

- Cybersource Hosted Order Page and Virtual Terminal (Payment Gateway)
- Global Payments Network (Acquirer/Processor)
- Acteva (1 time and/or seasonal merchants)
- Monster Commerce (Shopping Cart)
- Trustwave (SAQs & Scanning)
- Several 3rd Party Applications, all PCI Compliant, hosted off-campus, using Cybersource as their Payment Gateway

Credit Card Processing Website

Credit Card Processing @ MIT

[Home](#)

[Credit Card Overview](#)

[Becoming a Merchant](#)

[Existing Merchants](#)

[Information for Developers](#)

[MIT Policies and Compliance](#)

[News and Events](#)

[FAQ](#)

[Contact Us](#)

[Site Map](#)

NEWS

[Cost of Data Breaches](#)

[Cards at Schools — Bank Risks](#)

MIT strives to accept credit card payments in an accurate and secure manner. It does not store, process, or transmit credit card information.

MIT staff and students who accept credit card payments are known as MIT merchants. They adhere to Payment Credit Industry compliance rules, present business plans describing their business needs, and confirm each year that they are following the compliance regulations. In this way, MIT ensures that it has the proper safeguards in place.

If you are interested in becoming an MIT merchant, learn what you have to do to get started, find out how to process payments and donations, learn what it means to be compliant according to the Institute's regulations, and stay up-to-date on what is happening in the business world today.

An [MIT certificate](#) is required to view this site.

Project Communication Plan

| Type of Communication | Frequency | Communication Avenue |
|------------------------------|-------------------------------|--|
| Core Team Meeting | Weekly | Minutes/Action Log |
| Individual Merchant Meetings | Scheduled individually | PCI / Project Awareness / Merchant Profile |
| Vendor Demos | Scheduled individually | Evaluation Criteria / Vendor Presentations |
| Renewal Letters | Once & reminders | Renewal Form |
| Merchant Breakfast | Once | Presentation / Return Info Cards |
| Sponsor Meetings | Monthly | Presentation |
| Audit Committee Meetings | As requested | Presentation |
| ASPCC | As requested | Presentation |
| Relationship Management Team | Beginning of imp phase | Presentation |
| IT Help Desk | Beginning of imp phase | Presentation |
| IS&T Publishing | Beginning of imp phase | Presentation |
| Merchant Group Meetings | Individually by rollout group | Presentation |

Project Statistics – Tracking Progress

| Merchant Conversion | | |
|---------------------|----------------|---------|
| Merchant Status | # of Merchants | Percent |
| Total Merchants | 128 | |
| De-Activated | 33 | 26% |
| New (7 Acteva) | 11 | 9% |
| Remaining Merchants | 106 | 83% |
| Registered/Config | 106 | 100% |
| GoLive | 40 | 38% |
| Self Assessment | 0 | 0% |
| Scanning | 0 | 0% |

Lessons Learned

- Although we were able to significantly reduce the scope of PCI Compliance at MIT, the scope of the project was significantly increased by a decision to change to a different Acquirer/Processor as part of the project.
- This decision was made in the interest of reducing merchant processing costs and improving reporting and monthly reconciliation.
- These two goals were not achieved and the scope of the project increased significantly.

Situation at MIT Today

- Credit Card Processing Policies and Procedures Published
- Incident Response Policy Published / Team Named
- Credit Card Processing Website Published
- Merchants converted to Cybersource HOP in test (production by 6/30)
- Published Process for New Merchants
- Defined Process for Seasonal Merchants
- PCI Compliance for all 3rd Party Applications
 - ◆ Interfaced to Cybersource
- Established Support Model
- Minimized Paper Storage of Credit Card Information
- Minimized the Number of Credit Card Solutions
- Implemented a Self Assessment Process
- Established ongoing Relationships with Credit Card Partners
- Established Project & Administrative Website for Support Model
- **Eliminated the Need for PCI Scanning**

Q & A

Thank You

Contact Info:

Sandy Pata

spata@mit.edu or sandy_pata@msn.com

617-324-8981 or 508-572-9605

Merchant-services-core-team@mit.edu