Campus Credit Card Breach

IT 6/26/12
The Payment Card Industry Data Security Standard (PCI DSS) require that **ALL** companies **processing, transmitting, and/or storing** credit card information maintain a secure environment. Essentially any business unit with a Merchant ID (MID).
Three Basic Type of Breaches

* Physical Breach – theft of documents or equipment
* Electronic Breach – electronic breach of a system or network environment
* Skimming – capture of card magnetic stripe data using an external device
Costs of Non-PCI compliance

* Visa charges up to $50,000 penalty for first time offense
* MasterCard up to $2,000 penalty
* All fraud losses perpetrated using the account numbers associated with the compromise (from date of compromise forward)
* Cost of re-issuance of cards associated with the compromise (approximately $25 per card).
* Estimated maximum cost of HDRS data compromise - $6.8M
Non-PCI Compliance Costs

* Any additional fraud prevention/detection costs incurred by credit card issuers associated with the compromise (i.e. additional monitoring of system for fraudulent activity).
* Additional fines related to the violation of improper storage of Cardholder data up to $500,000.
* Forensic Expert Review - $18K+
* Loss of Customer Confidence
* Damage to reputation of the University
* Time and resources
Prior Campus Focus

- Internet transactions; encouraging use of campus gateway
- Coordination of new merchant ids
- Coordination of exceptions
- New vendor software
- Annual Cash Reviews
- PCI questionnaire completion
- Campus Data Security Review
Lessons Learned

* Respond to reports of suspected fraud immediately
* Software used with registers
* Share information with others
What you can do?

* Immediately report any suspected fraud to our Campus Credit Card Coordinator, Asirra Suguitan
* Communicate expectation that it is critical for customer data to be protected
* SAQ – Security Awareness Questionnaire
  * Ensure you have the right person certifying the questionnaire
    * Level of person signing (PCI requires Executive Officer)
    * Knowledge of PCI and your operations
    * Involve your technical experts
    * Vulnerability Scans (note: IT should have access to portal to monitor and read scans)
What you can do?

* SAE – Security Awareness Training
  * All staff with any involvement with credit cards must be trained
  * Including but not limited to:
    * Managers/Directors/Supervisors
    * Cashiers
    * Staff responsible for reconciliations
    * IT staff responsible for system setup and maintenance
    * Anyone with access to credit card information or with responsibilities over a campus merchant
What you can do?

* Using a third party service provider
  * Online or face-to-face transactions
  * Risk to University’s reputation whether using campus issued merchant ID or not
  * Use of a third part vendor is an exception to policy
  * Depending upon payment terms, may require OP approval
  * Vendor must be PCI certified annually and maintain PCI certification throughout the year
  * Provide network diagram of payment process and security to Campus Credit Card Coordinator, Asirra Suguitan
What are the campus post mitigation efforts?

* Partnering with C&C to have all campus merchants systems reviewed
* Campus Merchant meeting-February 2012
* Campus Merchant Credit Card meeting for IT personnel-June 2012
* All integrated registers now require external penetration testing as part of PCI process
* Internal penetration testing will now be performed by C&C
What is the campus doing?

* PCI compliance clause in purchase agreements will be required for Third party servicer providers
* Gap Analysis by external vendor
* Enhanced campus policy, procedure, best practices
  * Incident Response Team
  * Virtual Private Networks
  * PCI questionnaire
* Cash control review by OP consultant
Questions?