PCI Best Practices and Lessons Learned

Some Best Practices

- NEVER e-mail credit card information
- NEVER store credit card numbers in any database or spreadsheet
- Truncate all but last 4 digits of cc number
- Keep credit card documentation locked in a safe or filing cabinet
- Permit only employees who have a legitimate “need-to-know” access to cardholder info
- Destroy documentation containing credit card information when no longer needed for business or legal reasons
- Document departmental desktop procedures
- Update cash handling procedures
- Segregate duties – the individual performing reconciliation should not be involved in processing credit card sales or refunds

Compliance Is Not:

- Just a quarterly scan
- Just a signed SAQ
- Just anti-virus and complex passwords
- Vendors saying they are compliant

Compliance Is:

- Annual training for EVERYONE who transmits, stores or processes credit cards with “sign off”
- Redacting credit card information after the payment is processed
- Keeping credit card swipe machines in a secure place
- Certifying that all third party vendors involved in processing, transmitting or storing credit card information are PCI DSS compliant on a quarterly basis.

Things to Look For:

- Inadequate segmentation between card holder environment and campus network
- Inadequate inventory documentation
- Inconsistent forms management and storage
- Inadequate policies and procedures
- Annual training not performed
- Inadequate system scans
- Third party contracts need to be amended to include PCI compliance
- How cards are used in the development office
- Email used for registration and CHD
- Phone call transactions written on sticky notes
- CHD received via voice-mail messages
- CHD processed on forms, left on receptionist desk until they are hand delivered to cashier
- Forms with CHD “ripped up and thrown in the trash”
- Off-hours book sales handled by faculty – who complete forms and turn in to the bookstore
- Receipts stored in unlocked cabinets and large bins
- Keys to file cabinet kept in unlocked desks
- Shared accounts (passwords) in use
- CHD received via phone calls, written on a form and then entered into bank system via touch tone phone - forms then stored in the desk in the office
- CHD stored in boxes in an open area where classes are held