Information Technology Update

Tom Jackson
Vice Chancellor for Information Technology and Chief Information Officer

BOT Presentation

November 13, 2020

PCI Data Security Standard (DSS)

- PCI Data Security Standard
- Authentication
- IT Audit

PCI Data Security Standard

PCI Data Security Standard (DSS)

- Controls for processing credit and debit cards
- Compliance required by North Carolina Office of the State Controller (OSC) contract
- Severe penalties for non-compliance
- Does not fit the needs of an academic and research network
  - Very stringent and **restrictive**
- Controls depend on the methods used to collect and process card data

PCI DSS Assessment

- Identify each office processing credit or debit cards
- Identify the appropriate set of controls for each merchant ID
- Assessment Results
  - Merchant IDs: 22
  - Card Present: 18
  - E-commerce: 10
  - Analog Phone: 1
  - Mail Order: 2
  - Fax: 1
  - VoIP Phone: 8

PCI DSS Assessment

- VoIP Phone use puts the entire university network in scope for compliance
  - Conflicts with the needs of an education and research network
- Strategy
  - Outsource compliance
  - Remove card data from the university network
  - Reduce scope of compliance
  - Increase role of ITS in managing the technical aspects of compliance
- DSS Assessor Recommendations
  - Use P2PE devices to reduce scope
  - Not clear how this will remove VoIP Phones from scope

Authentication

Authentication Standard

- Approved in FY20
- Requires
  - Longer passwords
  - Authentication via OneID
  - Use of multifactor authentication (MFA)

Authentication Upgrades

- Banner Admin Pages
  - Moved to OneID with MFA in September 2018
- Banner Self Service
  - Moved to OneID in September 2020
  - Employees will move to MFA, pending registration
- OneID
  - Employees will move to new password requirements in November and December 2020
  - Concurrently, employees will register for Azure Self Service Password Reset (SSPR) and Azure MFA
- Office365
  - Employees will move to MFA pending registration

IT Audit

Audit Preparation Strategy

- Identify risks
  - Information Security Assessments FY19
  - Penetration Tests FY19 and FY20
  - Vulnerability Scanning
- Prioritized plan to address risks
  - Annual Security Plans FY19, FY20, and FY21
- Show progress towards addressing risks
  - Annual Security Plan FY19 and FY20 outcomes

Audit Focus

- Controls over student data
- Six areas
  - Hardware Inventory
  - Software Inventory
  - Vulnerability Management
  - Configuration Management
  - Administrative Privileges
  - Audit Logs
- These are the first six Center for Internet Security (CIS) controls
  - Overlap but distinct from ISO 27002 controls
  - More prescriptive and detailed

IT Audit Timeline

- November – December 2020: audit field work
- January – April 2021: analysis and report preparation
- May 2021: draft report

Data Exposure

Questions?