

*Auditing
the
Payment Card Industry
Data Security Standard
(PCI DSS)*

Presented By: Sean Edgar
Information Systems Auditor
Legislative Audit Division
State of Montana

Where did we get the idea?

- Detailed PCI DSS presentation at 2008 NSAA IT conference
 - Brian Rue, Assistant Director, Information Security, Florida State University
 - Led to our decision to conduct our audit
 - Information Systems conducted audit because it pertains to data security
- Recent major breaches
 - TJX
 - Heartland

[PCI DSS]

- Association created
 - Payment Card Industry Security Standards Council
- Standard developed (PCI DSS)
 - Twelve overarching standards
 - Creation of security policies, encryption of data, cardholder data storage and retention, etc.
 - Subdivided into many smaller sub-elements



Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall and router configuration standards that include the following:	1.1 Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.			
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	1.1.2.a Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks. 1.1.2.b Verify that the diagram is kept current.			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	1.1.3 Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. Verify that the current network diagram is consistent with the firewall configuration standards.			
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	1.1.4 Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.			

[Who should we audit?]

- Identified two contracts for payment card processing
 - State Web Portal Developer
 - Certified PCI DSS compliant
 - Cybertrust Certified
 - Processor for all other transactions
 - Used transaction information provided by processor
 - Identified top four agencies which accounted for 92% of non-web portal revenues

[Obligation to follow PCI DSS]

- MT has an exclusive term contract with processor
 - Contract requires the State to “comply with all security standards and guidelines that may be published from time to time by Visa, MasterCard, or any other Association”
 - PCI DSS is the “security standard”
 - Contract states each agency responsible for following contract terms
 - As a result we determined state agencies are required to follow PCI DSS

[Audit Objective]

- Determine if policies and business processes at selected entities conform to specific requirements of the PCI DSS.
 - Not a PCI DSS compliance audit as we are not Qualified Security Assessors (QSA's).
 - Not a full PCI DSS audit due to number of sub-elements and technical knowledge required.

[What should we audit?]

- Visited each of the four agencies
 - Identified business processes in place for accepting payment cards
 - Identified specific elements of the PCI DSS as criteria based on the business processes
- Three primary business processes
 - Paper
 - Point of Sale (POS)
 - Web

[Paper Based Transactions]

- Ensure paper based transactions are conducted with controls in place which enable agencies to conform to applicable elements of the PCI DSS.
 - PCI DSS Requirements
 - 3.1
 - 3.2
 - 3.3
 - 7.1
 - 9.1

[Paper Based Transactions]

- PCI DSS 3.2 states “Do not store sensitive authentication data after authorization (even if encrypted).”
 - Two agencies storing the sensitive authentication data, primary account number, cardholder name, address, and signature on forms.
 - One of these processed and stored the forms in an open environment.

[Paper Based Transactions]

- PCI DSS 9 states “Restrict physical access to cardholder data.”
 - Processing forms with cardholder information in open office environments
 - Cardholder information on yellow, sticky notes
 - Forms stored in unlocked locations or in open boxes

[POS Devices]

- Ensure payment card transactions are authorized through a direct link with the processor or they are encrypted. Determine if agencies have a complete listing of all POS machines in use.
 - PCI DSS Requirements
 - 4.1
 - 12.3

[POS Devices]

- Determine if agencies have a complete listing of all POS devices in use. (PCI DSS Req. 12.3.)
 - Requirement mandates development of “usage policies for critical employee facing technologies...” and the policy should include “a list of all such devices...”
 - None of the audited agencies had an inventory of POS devices at the planning stage.
 - 2 later produced inventories during fieldwork
 - 2 did not need them, limited # of devices

[POS Devices]

- Requirement 4.1 of the PCI DSS state “Use strong cryptography and security protocols... to safeguard sensitive cardholder data during transmission over open, public networks.”
 - Agencies using old machines, one from 1986
 - One model was reportedly easy to compromise

[Web Applications]

- Requirement 6.3 of the PCI DSS states “Develop software applications in accordance with the PCI DSS... and based on industry best practices.”
 - Developer certified PCI DSS compliant or
 - Application certified PCI DSS compliant
- All Web Application developers we reviewed were certified compliant

[Recommendation #1]

- Develop and implement security policies
 - Cardholder data retention
 - Storage of sensitive authentication data
 - Securing (masking) primary account numbers
 - Restricting access to cardholder data
 - Completing and tracking an inventory of all point of sale devices
- Communicate security policies to staff
- Monitor implementation of security policies

[Recommendation #2]

- Ensure all point of sale devices encrypt cardholder data as required by the Payment Card Industry Data Security Standard.

[Agency Reaction]

- Who is responsible for policy?
 - Individual agencies or Dept. of Administration
 - Contract acquirer or cardholder data owner
 - We determined agencies are responsible
- What is an open, public network?
 - Are telephone lines open, public networks
 - Never received clarification from PCI Security Council
 - Erred on the side of data security

[Audit Outcomes]

- Performance Audit has scheduled audit of Dept. of Administration Contracting
- Legislative Audit Committee directed Legislative Audit Division to inform all agency directors of report findings.
- 9/1/09: new Statewide Online Payment Processing Policy effective.
 - Requires compliance with PCI DSS

[*Payment Card Industry Data Security Standard and Related Controls*]

Questions?

<http://leg.mt.gov/content/Publications/Audit/Report/09DP-02.pdf>