

Payment Card Industry Data Security Standard

Mark K. Mellis, CISM
President, Mellis and Associates, Inc.

What we'll cover

- * History
- * Impact
- * What it is
- * How it is Enforced
- * War Stories
- * Questions

History of the PCI DSS

- * VISA, Mastercard, American Express, Discover, and JCB all had their own security programs
- * Formed the Payment Card Industry Security Standards Council in late 2004 and issued version 1.0 of the PCI DSS
- * Version 1.1 issued in September 2006

Impact of PCI DSS

- * huge impact on the industry
- * prescriptive, not like other standards
- * teeth behind it: fines, rate increases, potential loss of the ability to process credit card transactions

What it is

- * Part of a family of standards
 - * PIN Entry Device Standard
 - * Payment Application DSS
- * Six Control Objectives
- * Twelve Requirements

Build and Maintain a Secure Network

- * Install and maintain a firewall configuration to protect cardholder data
- * Do not use vendor-supplied defaults for system passwords and online security parameters

Protect Cardholder Data

- * Protect stored cardholder data
- * Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- * Use and regularly update anti-virus software or programs
- * Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- * Restrict access to cardholder data by business need-to-know
- * Assign a unique ID to each person with computer access
- * Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- * Track and monitor all access to network resources and cardholder data
- * Regularly test security systems and processes

Maintain an Information Security Policy

- * Maintain a policy that addresses information security for employees and contractors

How it is Enforced

- * Self Assessment Questionnaire
 - * if you store CHD, 226 questions
- * Required Scans
 - * Authorized Scanning Vendor, quarterly
- * Attestation of Compliance

War Stories - CISO

- * In some ways it is like an introductory security tutorial
- * “Do that stuff, you’ll be good.”
- * Incident several years ago
 - * followed incident response plan to the letter, good policies and procedures, no fine

War Stories - Application Architect

- * High Volume Application
- * Audit every year, "trust but verify"
- * looked through all logs for PAN
- * reviewed encryption policies, looked through database tables for clear-text PAN

War Stories - QSA President

- * Good system architecture can limit the scope and expense of compliance
- * System inspection depends on the assessor - you get what you pay for
- * \$20,000 to play, plus \$1,250 per initial employee, \$995 per year afterwards
- * QSAs must be CISSP, CISA, CISM

War Stories - QSA

- * DSS has teeth
- * Training and exam are focussed on DSS, not on security; exam not trivial
- * Prescriptiveness of standard ensures apples-to-apples evaluations, but hands-on component of assessments are notoriously subjective

Resources

- * <https://www.pcisecuritystandards.org>
- * <http://systemexperts.blogspot.com>