The PCI Security Standards Council

• An open global forum, launched in 2006, responsible for the development, management, education, and awareness of the PCI Security Standards, including:
  – Data Security Standard (DSS)
  – Payment Application Data Security Standard (PA-DSS)
  – Pin-Entry Device (PED)
PCI DSS Drivers

Advisory Board

Industry Best Practices

Community Meeting

Proactive feedback from Participating Organizations Community

PCI Data Security Standard

Approved Scanning Vendors (ASVs) and Qualified Security Assessors (QSAs)

ADC Forensics Results

Security Scans

On-Site Audits

Self-Assessment Questionnaire
Roles and Responsibilities of the Council

<table>
<thead>
<tr>
<th>PCI SSC...</th>
<th>PCI SSC Does Not...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Is an Independent Industry Standard</td>
<td>• Manage or drive Compliance</td>
</tr>
<tr>
<td>• Manages the technical and business requirements for how payment data should be stored and protected</td>
<td>– Each brand continues to maintain its own compliance programs</td>
</tr>
<tr>
<td>• Maintains List of Qualified PCI Assessors</td>
<td>• Identifies stakeholders that need to validate compliance</td>
</tr>
<tr>
<td>– QSAs, ASVs</td>
<td>• Definitions of Validation Levels</td>
</tr>
<tr>
<td></td>
<td>• Fines and Fees</td>
</tr>
</tbody>
</table>
2009 PCI SSC Objectives

- Manage new and existing standards
- Operational Stability and Efficiency
- Enhance Stakeholder Engagement
- Training
- Expand Global Reach of PCI SSC
**Global Headlines**

**The New York Times**

3 Indicted in Theft of 130 Million Card Numbers

**The Daily T**

Major Card Heist at Process

**Net.be**

Hacker pleads guilty to monster credit card theft

**The New Zealand Herald**

Hacker pleads guilty to monster credit card theft

**Global Headlines**

Hacker pleads guilty to monster credit card theft
WHAT WIVES SAY...

...go to the store; lay down the mulch; wash and wax the car; get the kids at school; rent some videos, and finish the rest of the dishes.

WHAT HUSBANDS HEAR...

...GO to the store; LAY DOWN the mulch AND GET some videos, and finish the rest of the dishes.
Did You Know?

According to Verizon’s 2009 Data Breach Investigations Report (DBIR)

- 75% of compromises were discovered at least weeks after the compromise.
- Post-breach reviews resulted in the discovery that:
  - Breached organizations only had 11% compliance level for Req 3 (Protect card holder data).
  - only 5% compliance level for Req 10 (track & monitor all access to network resources and cardholder data)
Changing a mindset
Common Myths of PCI DSS

- One product will make us compliant
- Outsourcing processing makes us compliant
- PCI DSS compliance is an IT project
- PCI DSS will make us secure
- PCI DSS is unreasonable; it requires too much
Common Myths of PCI DSS

• PCI DSS requires us to hire a QSA
• PCI DSS is only for high-volume transactions
• We completed a SAQ so we’re compliant
• We are required to store cardholder data
• PCI DSS is too hard
What’s Next?

1. Market Implementation (10/1/08–6/30/09)
2. Feedback Begins (7/1/09–10/31/09)
3. Feedback Review and Decision (11/1/09–4/30/10)
5. Discuss New Version / Revision (9/30/10)
What’s Next?

• Research of Emerging Technologies

• Special Interest Groups
  • Wireless
  • Virtualization
  • Pre-Authorization
  • Scoping

• New education programs

• Additional standards

• Quality Assurance program

• 2010 release of PCI DSS, PA-DSS and PTS