What are the threats to card data?

How can you defend your card data?

What is the Council doing to help you?

What tools are available to get you secure?

How can you be involved?
<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the threats to card data?</td>
</tr>
<tr>
<td>How can you defend your card data?</td>
</tr>
<tr>
<td>What is the Council doing to help you?</td>
</tr>
<tr>
<td>What tools are available to get you secure?</td>
</tr>
<tr>
<td>How can you be involved?</td>
</tr>
</tbody>
</table>
Why SECURITY matters…

“The attackers have changed with the emergence of organized crime into these cybercrimes...It's all about the money now ... Profit is driving these groups.” - FBI agent J. Keith Mularski, May 2009

According to Gartner, payment card fraud was the method most actively used by crooks to steal money, claiming 36 percent more victims in 2008 than other types of fraud. - Gartner, March 2009

There were more than 222 million potentially compromised records in 2009 - Identity Theft Resource Center Breach Report, Jan. 8, 2010

“Nearly twice as many people who lost money to fraud in 2008 changed their shopping, payment and e-commerce behavior,” said Avivah Litan, vice president and distinguished analyst at Gartner, March 2009

*Is your focus on compliance audits rather than security making you a target? Is your risky behavior potentially causing you to lose customers?*

**Remember, compliance is a byproduct of SECURITY**
According to Verizon’s 2011 Data Breach Investigations Report (DBIR)

79% of records were compromised through malware

2/3 of malware investigated was customized

79% of compromises were not discovered until, weeks, months or years had past

Data security is not all about prevention; it also requires detection and monitoring!
Breached organizations are 50 percent less likely to be PCI-compliant than a "normal population of PCI clients."

Top attack methods used to compromise payment card data:

- malware and hacking (25%)
- SQL injections (24%)
- exploitation of default or guessable credentials (21%)
Figure 3. Industry groups represented by percent of breaches

- Hospitality: 40%
- Retail: 25%
- Financial Services: 22%
- Government: 4%
- Manufacturing: 2%
- Tech Services: 2%
- Business Services: 1%
- Healthcare: 1%
- Media: <1%
- Transportation: <1%
- Other: 2%

Figure 4. Compromised records by industry group

- Retail & Hospitality: 56%
- Financial Services: 35%
- All Others: 9%
What are the threats to card data?

How can you defend your card data?

What is the Council doing to help you?

What tools are available to get you secure?

How can you be involved?
Payment Card Industry Security Standards
Protection of Cardholder Payment Data

Ecosystem of payment devices, applications, infrastructure and users
PCI compliant organizations suffer fewer data breaches
Organizations reporting compliance with the standards has increased tremendously over the last year
The volume of breaches reported in the Verizon DBIR decreased close to a hundredfold from their 2008 peaks

1. The Ponemon Institute’s 2011 PCI DSS Compliance Trends Study
Open, global forum

*Founded 2006*

Responsible for PCI Security Standards

- Development
- Management
- Education
- Awareness
More than 600 organizations have joined

North America: 480
Europe: 96
Asia Pacific: 33
Central Europe / Middle East / Africa: 17
Latin America / Caribbean: 8
What are the threats to card data?

How can you defend your card data?

What is the Council doing to help you?

What tools are available to get you secure?

How can you be involved?
Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 2.0
October 2010
Payment Card Industry (PCI)
Payment Application Data Security Standard

Requirements and Security Assessment Procedures
Version 2.0
October 2010
Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Point of Interaction (POI)

Modular Security Requirements
Version 3.0
April 2010
Your feedback has made the standard more mature and will help secure payment card data well into the future!
- Scoping
- Logging
- Risk-based approach
- Alignment between PA-DSS & PCI-DSS
- Recognition of small merchant environments
- New website and updated supporting documentation
What are the threats to card data?

How can you defend your card data?

What is the Council doing to help you?

What tools are available to get you secure?

How can you be involved?
PCI Security Standards Council

Overview of Changes to PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements for organizations that store, process, or transmit cardholder data. The standard is managed by the PCI Security Standards Council (PCI SSC). Changes to the standard are announced in new versions of the PCI DSS. This article describes the changes made in the latest version of the standard.

New Standard Published

- Makes new release of PINS
- Presented at Community Meetings in October
- Published in June
- Previous version remains effective for 12 months after the new standard becomes effective.

Stage 1: Start

Stage 1 starts on a new cycle, and a new lifecycle for the security of the cardholder data environment.

Stage 2: Feedback

Stage 2 is an opportunity for feedback on the new standard.

PCI Data Storage Do's and Don'ts

PCI Data Storage Do's and Don'ts

1. Do understand when payment card data is involved in the transaction process.
2. Do not store cardholder data in a way that is inappropriate.
3. Do ensure that cardholder data is stored securely.
4. Do not store cardholder data that is no longer needed.
5. Do not use cardholder data for marketing purposes.
6. Do not use cardholder data for other unauthorized purposes.
7. Do not sell or share cardholder data.
8. Do not distribute cardholder data.
9. Do not use cardholder data for any purpose other than the intended use.
10. Do not use cardholder data for any purpose other than the intended use.

PCI Data Storage Do's and Don'ts

1. Do understand when payment card data is involved in the transaction process.
2. Do not store cardholder data in a way that is inappropriate.
3. Do ensure that cardholder data is stored securely.
4. Do not store cardholder data that is no longer needed.
5. Do not use cardholder data for marketing purposes.
6. Do not use cardholder data for other unauthorized purposes.
7. Do not sell or share cardholder data.
8. Do not distribute cardholder data.
9. Do not use cardholder data for any purpose other than the intended use.
10. Do not use cardholder data for any purpose other than the intended use.
Who Should Attend?

Open to anyone who is interested in learning more about PCI, with a focus on those individuals working for organizations that must meet compliance with the PCI DSS or have a vested interest in the Payment Card Industry.

Upcoming Training Dates

August 24th, 2011 – Boston, MA, USA
PCI Awareness Training – Online!

• At your home or office, at your pace

• Offers general PCI training across your business to ensure a universal understanding of PCI compliance

• Provides **four** CPE hours

• Available all the time, anytime!

<table>
<thead>
<tr>
<th>Number of Employees Registered</th>
<th>Price Per Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 24</td>
<td>$495 USD</td>
</tr>
<tr>
<td>25 - 99</td>
<td>$395 USD</td>
</tr>
<tr>
<td>100+</td>
<td>$295 USD</td>
</tr>
</tbody>
</table>

Discounts are available for group registration. Please contact the PCI SSC Training Coordinator at training@pcisecuritystandards.org for more information.

https://www.pcisecuritystandards.org/training/non_certification_training.php
Security standards and supporting documents

Quick Reference Guide

Searchable Frequently Asked Questions

List of approved QSAs, ASVs, PA-QSAs, PED Labs

Education and outreach - e.g., fact sheets, webinars

Participating membership, meetings, collaboration

A global voice for the industry
Join us as a Participating Organization to get involved in setting global PCI standards!
Focus on security, not compliance

Understand the process of PCI standards development

Join us as a Participating Organization and increase our global presence

Take advantage of the Council’s resources and guidance

Participate in the 2011 Annual Community Meetings

Adopt version 2.0 and share the PCI SSC roadmap with internal stakeholders
Any Questions?

Please visit our website at www.pcisecuritystandards.org
What Did You Think?

In order to help us create/provide a better HITEC experience in the future, please take a second to fill out the short survey that will be sent to you via e-mail at the end of the day.

And THANK YOU for attending HITEC!

Learn how HFTP membership can benefit you, visit www.hftp.org