

# Overlooked PCI-DSS Compliance: People

May 20, 2009

8:15 a.m. – 9:15 a.m.

# Disclaimer

The opinions of the contributors expressed herein do not necessarily state or reflect those of the National Association of Convenience Stores. Reference herein to any specific commercial products, process, or service by trade name, trademark manufacturer, or otherwise, shall not constitute or imply an endorsement, recommendation, or support by the National Association of Convenience Stores. The National Association of Convenience Stores makes no warranty, express or implied, nor does it assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials.

## Presenter:

---



BJ Stephan  
Senior Security Consultant  
FishNet Security

## Moderator:

---



Dave Thompson  
Vice President – Global Engineering, Systems & Payments  
Dresser Wayne

# Payment Card Industry (PCI)

The Payment Card Industry (PCI) has designed a security framework with the intention of preventing the ever increasing amount of identity theft and credit card fraud. The framework is called the Payment Card Industry Data Security Standard (PCI DSS).



# PCI Cardholder Data (CHD)

The PCI Data Security Standard is a list of controls designed to help mitigate the risk of exposure of cardholder data.

Cardholder Data (CHD) – Information pertaining to the cardholder and cardholder's account.

- Account number
- CVV2
- Cardholder Name
- Expiration Date

# Personnel: Why should I worry about my staff?

# Examples of Some PCI Breaches

- Feb. 18, 2005**      **Atlantis Hotel**      Dishonest insider compromises 55,000 credit card numbers, social security numbers, addresses, and names.
- May 2, 2006**      **Georgia State Government**      Government surplus computers were sold before their hard drives were erased. The drives contained cardholder data, birthdays, social security numbers.
- Feb. 7, 2007** **Front Range Ski Shop**      The shop's Web site was broken into and customer information including credit card account data may have been accessed. (15,000 records)
- Feb. 19, 2007**      **Stop & Shop Supermarkets**      Credit and debit card account information including PIN numbers was stolen by high-tech thieves who apparently broke into checkout-line card readers and PIN pads and tampered with them.
- June 14, 2007**      **Hamburger Hamlet Restaurant**      Former waitress made off with the credit or debit card numbers of at least half a dozen patrons - and possibly as many as 40. Already, about \$16,300 in unauthorized charges have been linked to the scam.
- Jan. 20, 2009**      **Heartland Payment Systems**      After being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, the company last week found evidence of malicious software that compromised card data that crossed Heartland's network. This incident may be the result of a global cyber fraud operation.

# Pizza Cell Phone Scam

**Pizza delivery front counter cell phone camera exposure.**

- An individual was picking up his pizza order. The clerk asked for his credit card and he gave it to him to swipe. The clerk swiped the card then set it on the counter. While the card was processing the clerk acted like he was receiving or sending a text message. The customer heard a click and realized the clerk wasn't texting but rather taking a photo of his credit card that the clerk put on the counter.

# Prevention

- Cardholder Data (CHD) pertains to any information on the physical card itself or the magnetic strip.
- Physical access to CHD is often overlooked when addressing even the most simple procedures.
  - Do you need access?
  - Can the card swipe be moved to prevent the card from leaving the customers hand?
  - Who has the card while the device is “dialing” out to complete the transaction?
  - 12.6: Implement a formal security awareness program to make all employees aware of the importance of CHD security.

# Security Awareness Training

All individuals with access to cardholder data must received formal security awareness training no less that once a year.

- Examples:
  - Sales clerks (receive the card from the client to run on the register)
  - Managers with access to backend servers
  - Corporate employees
  - Database engineers
  - Janitorial staff with access to managers office (receipts and servers)

# E-Commerce QA CHD Theft

**Internal QA breach by individual with legitimate business requirement.**

- An E-Commerce company in Arizona had a breach of cardholder data. An individual in the Quality Assurance department was taking credit card numbers and running up large transactions through online purchases.
  - The FBI arrested the individual at the office during business hours.

# Business Requirements for CHD

- If an individual is given access to CHD you must always ask:
  - Why?
  - Is that access required?
  - Can their job be completed with partial access (first six or last four)?
- Who is the person receiving access
  - Have you completed a background check?
    - 12.7: Screen potential employees prior to hire to minimize the risk of attacks from internal sources.
  - What is “their” liability or responsibility to CHD?
  - Are “they” aware of their responsibility?
    - If so do you have proof of “their” awareness and acceptance in writing?

# CHD Breach

## What do I do if I discover I have had a breach of CHD?

- 1) Stay calm
- 2) Initiate your Incident Response Program
- 3) Escalate to the proper internal management
- 4) Get legal counsel involved ASAP
- 5) Do not make rash decisions. This can lead to corruption / contamination of evidence or further propagation of the breach.
- 6) Notify the card brands as quickly as required.
  - Consult with legal counsel to determine reporting requirements for both the card brands and local authorities.
- 7) Be prepared to engage a Qualified Incident Response Assessor (QIRA) ASAP.
- 8) Follow VISA's breach guidelines:
  - [http://usa.visa.com/download/merchants/cisp\\_what\\_to\\_do\\_if\\_compromised.pdf](http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf)

**PCI compliance is NOT just about hardware.**

# Common Potholes

- Potholes Observed:
  - No Antivirus
  - Insufficient password policy
  - Shared user accounts
  - Un-patched systems
  - Insecure Internet access
  - Failure to secure paper printouts
    - Proper shredding
  - Lack of formal policies and procedures
  - No security awareness training

# Antivirus

**5.1: Deploy anti-virus on all systems commonly affected by malicious software (particularly personal computers and servers).**

- What is considered “commonly affected”?
  - Rule of thumb: If there is an AV available for that system / platform, then you must have AV installed.
- Antivirus also implies that the software is able to detect and remove all types of malicious software (spyware, adware, rootkits, worms, trojans, etc).

# Password Policy

## 8.5: Ensure proper user authentication and password management for non-consumer users and administrators on all system components.

- Required:
  - Reset after 90 days
  - Must be complex (numeric and alphabetic)
  - Minimum of 7 characters
  - 4 password history
  - Accounts are locked out after 6 invalid attempts
  - Locked accounts remain locked for 30 min or until reset by an admin
  
- Recommended:
  - Do not write down passwords
  - Do not put passwords on a sticky note on the monitor or under the keyboard
  - Do not share passwords with anyone (including your auditor, even if they ask)
  - Do not use dictionary words
  - Do not replace letters with corresponding numbers or symbols ('@dm!n', 'l3t\_m3\_!n', 'h3110w0rld')

# Physical Media

**9.10.1: Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.**

- What does this mean?
  - Do you have receipts with full PAN?
  - Do you shred receipts when no longer needed?
  - Do I have to use a third party shredding company?
    - No, self certified shredding
  - Do you print out reports with PANs on them?
  - What other physical media has PANs on them?
  - Is your managers office locked at all times?
  - Are reports and receipts stored in a locked cabinet?

# Policies and Procedures

**The PCI DSS requires multiple policies and procedures. How do I fulfill this requirement? Where can I find help?**

- There are 4 key policies that are required in almost every PCI audit:
  - Security Policy
  - Change Management Policy
  - Software Development Life Cycle
  - Incident Response Policy
- SANS.org provides free policy templates:
  - <http://www.sans.org/resources/policies/>
- Join you local security chapters and ask others to help you:
  - [www.issa.org](http://www.issa.org)
  - [www.isaca.org](http://www.isaca.org)
  - [www.infragard.org](http://www.infragard.org)

# Questions?



Benjamin Stephan

[BJ@fishnetsecurity.com](mailto:BJ@fishnetsecurity.com)

**Thank you!**