PAYMENT CARD INDUSTRY (PCI) COMPLIANCE – HISTORY & OVERVIEW

David Kittle – Chief Information Officer
Chris Ditmarsch – Network & Security Administrator

Smoker Friendly International / The Cigarette Store Corp

8/21/2014

What is PCI Compliance (PCI DSS)?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that *ALL* companies that **process, store, or transmit** credit card information maintain a secure environment. If you have a Merchant ID, you need to be PCI DSS compliant!

The History of PCI Compliance…

Between 1988 and 1998, Visa and MasterCard reported credit card fraud losses totaling 750 million dollars. This is a tiny amount compared to the hundreds of **billions** of dollars in transactions processed during the same time period.

The Internet era changed all of that…

The History of PCI Compliance…(cont'd)

- Late 1990s
  - Internet era begins; spawns new avenues for payment card fraud.
- October 1999
  - Visa approves Cardholder Information Security Program. CISP is the first of several precursors to the PCI DSS.
- Early 2000s
  - Online credit card fraud grows. In 2000, CyberSource reports that online revenue lost due to payment card fraud reached $1.5 billion. It would nearly triple throughout the course of the decade.
- May 2001
  - Visa and other card brands struggle to enforce security policies. Few companies are able to fully meet Visa's May 1, 2001, CISP compliance deadline due to disparities between Visa's North American and international guidelines. Guidelines from other card brands are less successful because of the lack of a unified standard.
- July 2004
  - Web infrastructure attacks become rampant. Malware, such as key loggers and Trojans are now being used to steal cardholder data.
- December 15, 2004
  - PCI DSS 1.0 Debuts. Compliance is mandatory for merchants and any other organization in the payment lifecycle.
- September 2006
  - The PCI Security Standards Council is formed and PCI DSS 1.1 is released (addressing web application issues)
- October 2008
  - PCI DSS 1.2 released. Addresses 802.1x wireless issues estimated to cost merchants millions of dollar to implement.
- October 2010
  - PCI DSS 2.0 released. No major changes in this release. Verizon releases it's own PCI Industry Compliance Report finding that companies struggle "mightily" to meet and maintain PCI DSS compliance.
- November 2013
  - PCI DSS 3.0 released. Emphasizes the need for in-house vulnerability assessments and the integration of compliance best practices into day-to-day business operations.

What is The Payment Card Industry Security Standards Council (PCI SSC)?

- The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.).
- Launched in September, 2006
- The council's purpose is to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process.
- It is important to note, the payment brands and acquirers are responsible for enforcing compliance, not the PCI council.

To whom does PCI apply?

- PCI applies to *ALL* organizations or merchants, *regardless of size or number of transactions* that accepts, transmits or stores any cardholder data. Simply said, if any customer ever pays you directly using a credit or debit card, then PCI DSS requirements apply.

Where can I find the PCI Data Security Standards (PCI DSS)?

- The standard can be found on the PCI SSC's website.
- https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

What are the PCI compliance deadlines?

- If you store, process or transmit cardholder data, you must be compliant now. However, if you are a Level 4 merchant, you will have to refer to your merchant bank for their specific validation requirements and deadlines. All deadline enforcement will come from your merchant bank. You may also find more information on Visa's website:
- http://usa.visa.com/download/merchants/payment_application_security_mandates.pdf.

What are the PCI compliance ‘levels’ and how are they determined?

- All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant.
- In cases where a merchant corporation has more than one DBA (Doing Business As), Visa acquirers must consider the aggregate volume of transactions stored, processed or transmitted by the corporate entity to determine the validation level. If data is not aggregated, such that the corporate entity does not store, process or transmit cardholder data on behalf of multiple DBAs, acquirers will continue to consider the DBA’s individual transaction volume to determine the validation level.

What are the PCI compliance 'levels' and how are they determined? (cont'd)

Merchant Level	Description
1	Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant — regardless of acceptance channel — processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	**Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year.**

** Any merchant that has suffered a hack that resulted in an account data compromise may be escalated to a higher validation level.*

Source: *http://usa.visa.com/merchants/risk_management/cisp_merchants.html*

How does a small-to-medium sized business (Level 4 merchant) satisfy the PCI requirements?

- To satisfy the requirements of PCI, a level 4 merchant must complete a Self Assessment Questionnaire (SAQ):
  - First, identify your Validation Type as defined by PCI DSS – see below . This is used to determine which Self Assessment Questionnaire is appropriate for your business.

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*	A
2	Imprint only merchants with no cardholder data storage.	B
3	Stand-alone dial-up terminal merchants, no cardholder data storage.	B
4	Merchants with payment application systems connected to the Internet, no cardholder data storage.	C
5	All other merchants (not included in descriptions for SAQs A-C above) and all service providers defined by a payment brand as eligible to complete an SAQ.	D

How does a small-to-medium sized business (Level 4 merchant) satisfy the PCI requirements? (cont'd)

- Complete the Self-Assessment Questionnaire according to the instructions in the Self- Assessment Questionnaire Instructions and Guidelines.
- Complete and obtain evidence of a passing vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV).
  - **Note:** scanning does not apply to all merchants. It is required for Validation Type 4 and 5 – those merchants with external facing IP addresses. Basically if you electronically store cardholder information or if your processing systems have any internet connectivity, a quarterly scan by an approved scanning vendor is required.
- Complete the relevant Attestation of Compliance in its entirety (located in the SAQ tool).
- Submit the SAQ, evidence of a passing scan (if applicable), and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

How does a small-to-medium sized business (Level 4 merchant) satisfy the PCI requirements? (cont'd)

- I'm a small merchant with very few card transactions; do I need to be compliant with PCI DSS?
  - All merchants, small or large, need to be PCI compliant. The payment brands have collectively adopted PCI DSS as the requirement for organizations that process, store or transmit payment cardholder data.

Other General Questions…

Q: If I only accept credit cards over the phone, does PCI still apply to me?
A: Yes. All businesses that store, process or transmit payment cardholder data must be PCI Compliant.

Q: Do organizations using third-party processors have to be PCI compliant?
A: Yes. Merely using a third-party company does not exclude a company from PCI compliance. It may cut down on their risk exposure and consequently reduce the effort to validate compliance. However, it does not mean they can ignore PCI.

Q: My business has multiple locations, is each location required to validate PCI Compliance?
A: If your business locations process under the same Tax ID, then typically you are only required to validate once annually for all locations. And, submit quarterly passing network scans by a PCI SSC Approved Scanning Vendor (ASV), if applicable.

Q: Are debit card transactions in scope for PCI?
A: In-scope cards include any debit, credit, and pre-paid cards branded with one of the five card association/brand logos that participate in the PCI SSC – American Express, Discover, JCB, MasterCard, and Visa International.

Q: What is defined as 'cardholder data'?
A: Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.

Other General Questions…(cont'd)

Q: Do I need vulnerability scanning to validate compliance?
A: If you electronically store cardholder data post authorization or if your processing systems have any internet connectivity, a quarterly scan by a PCI SSC Approved Scanning Vendor (ASV) is required.

Q: How often do I have to scan?
A: Every 90 days/once per quarter you are required to submit a passing scan. Merchants and service providers should submit compliance documentation (successful scan reports) according to the timetable determined by their acquirer. Scans must be conducted by a PCI SSC Approved Scanning Vendor (ASV).

Q: What is a network security scan?
A: A network security scan involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan will identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network. The Approved Scanning Vendors (ASV's) tool will not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks will be performed.

Note, typically only merchants with external facing IP address are required to have passing quarterly scans to validate PCI compliance. This is usually merchants completing the SAQ C or D version.

Q: What if a merchant refuses to cooperate?
A: PCI is not, in itself, a law. The standard was created by the major card brands such as Visa, MasterCard, Discover, AMEX, and JCB. At their acquirers/service providers discretion, merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, brand damage, etc., should a breach event occur.

What are the penalties for non-compliance?

- The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine on downstream till it eventually hits the merchant.
- Furthermore, the bank will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business.
  - It is important to be familiar with your merchant account agreement, which should outline your exposure.

Payment Card Industry Data Security Standard (PCI DSS)

What is it and why do we need it?

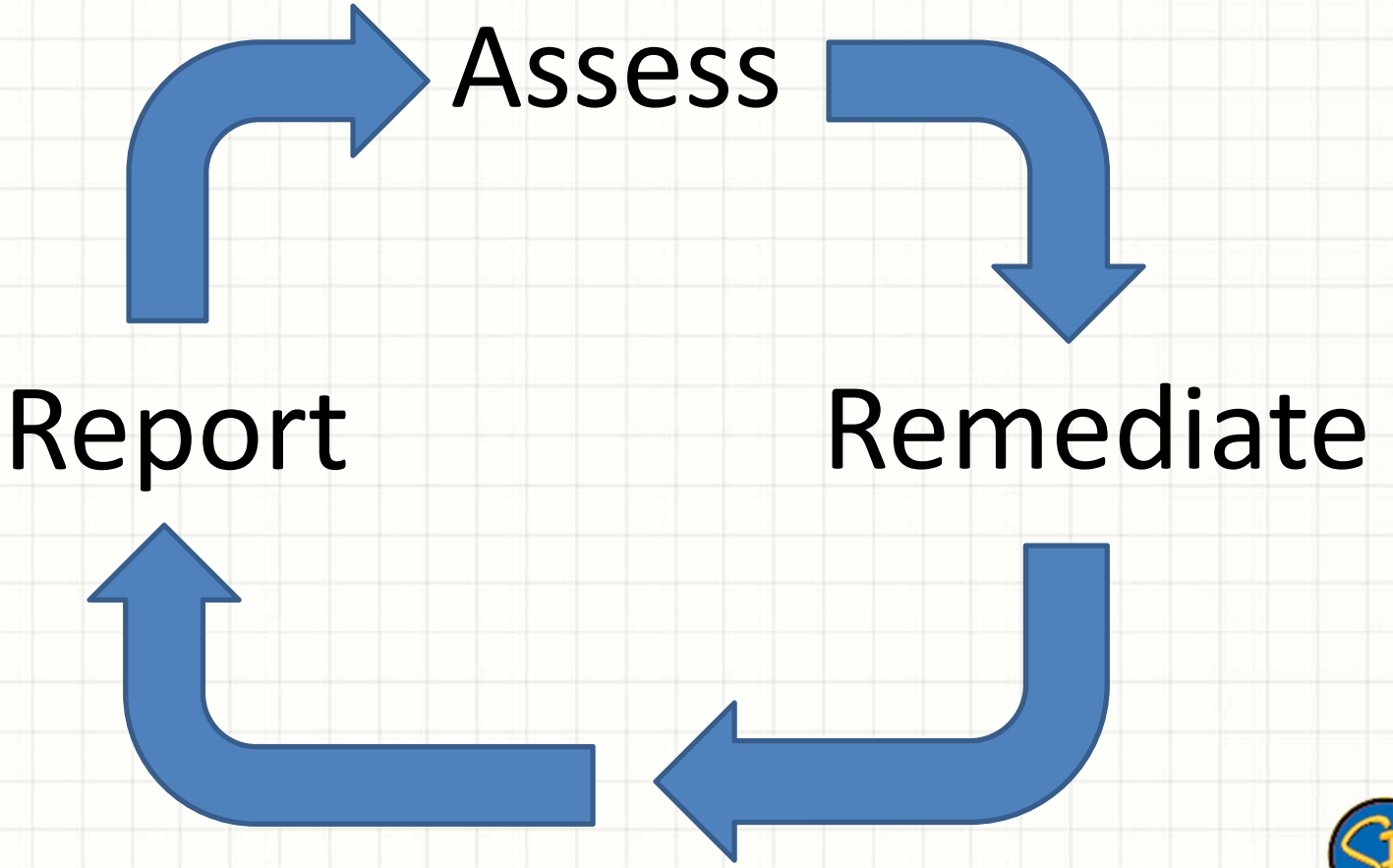
The PCI DSS is a set of common sense steps that mirror best security practices.

You should be adhering to these steps, even if they were not required!

How do we protect cardholder data and make sure we are in compliance with PCI DSS?

Assess -> Remediate -> Report

PCI DSS Compliance is a Cycle…



- # Assess
  - Identifying cardholder data, taking inventory of all your IT assets and business processes for payment card processing and analyzing them for vulnerabilities that could expose card holder data.
- # Remediate
  - Fix vulnerabilities.
  - Ensure you are not storing cardholder data unless there is a strong business case for doing so.
  - If there IS a business case for storing cardholder data, be prepared to fully document and back up that need.
- # Report
  - Compile and submit required remediation validation records (if applicable), and submit compliance reports to the acquiring bank and card brands with which you do business.

What are the goals of the Payment Card Industry Data Security Standard (PCI DSS)?

Goal	Basic Requirement(s)
Build & Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect cardholder data stored on your network and other systems under your control. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Assign and maintain a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor & Test Networks	10. Track & monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

What to Secure?

- Focus on protecting cardholder data under your control.
- You are responsible for protecting cardholder data at the point of sale, and as it flows into the payment system.
- The best step you can take is to not store cardholder data in any form.

Where Can Cardholder Data be Compromised?

- Credit Card Readers
- Point of Sale Systems
- Store Networks & Wireless Access Points/Routers
- Payment Card Data Storage* and Transmission
- Payment Card Data Stored in Paper-based Records
- Employees

* DON'T DO IT!

What Else?

- PCI Scope
  - Determine what system components are governed by PCI DSS. This is determined by evaluating where in your system cardholder data is stored and/or transmitted.

Thank You!

For more information regarding PCI Compliance, please visit the Payment Card Industry Security Standards Council website at:

http://www.pcisecuritystandards.org