LBMC INFORMATION SECURITY

PCI Compliance
Pitfalls and Challenges

Stewart Fey, CISA, CISSP,QSA

Agenda

- PCI DSS Overview
- PCI's 12 Requirements
- The Cardholder Data Environment
- Common PCI DSS Compliance Challenges
- PCI 3.2

LBMC INFORMATION SECURITY

Who's the next headline…

LBMC INFORMATION SECURITY

Setting the Stage

Why and what do I know about PCI?

- Qualified Security Assessor (QSA)
- Involved in PCI since the standard was first formed.
- Conducted PCI assessments for all types of organizations and government entities

LBMC INFORMATION SECURITY

What is PCI?

- Commonly called PCI DSS – Stands for: "Payment Card Industry Data Security Standard"

- Industry security rules set by the major card brands to protect credit card information.

LBMC INFORMATION SECURITY

Background of PCI

- Prior to 2004 each card brand had its own security requirements that each merchant (knowingly or unknowingly) agreed to abide by.
- No real enforcement or reporting structure in place. Most merchants were unaware of such requirements.

Background of PCI

- In 2004 the credit card industry agreed on a single information security standard

Payment Card Industry Data Security Standard (PCI DSS).

  - Visa: CISP Program
  - MC: Site Data Protection (SDP)
  - Amex: Data Security Operating Policy (DSOP)
- The PCI Security Standards Council was created in 2006 to oversee the PCI compliance process
  - Responsible for development, management, education, and awareness of PCI DSS

LBMC INFORMATION SECURITY

PCI: Good News & Bad News

- Compliance is rigorous.
- Many companies struggle to comply.
- PCI is not a law, so the government is not involved in enforcement.
- The PCI standard provides more granular prescriptive guidance than government standards like HIPAA or GLBA.

LBMC INFORMATION SECURITY

Who Are the PCI Players?

- **The Payment Brands**
  - American Express, Discover, JCB, MasterCard, and VISA
  - Define compliance programs and enforcement
  - Assess fines & penalties

- **PCI Security Standards Council**
  - Maintain the PCI DSS standard
  - Gatekeepers for Qualified Security Assessor (QSA) and other PCI certifications

LBMC INFORMATION SECURITY

Who Are the PCI Players (con't)?

- **Acquirers (Merchant Bank)**
  - Processes merchant payment card transactions
  - Responsible for merchant compliance with PCI DSS

- Qualified Security Assessor (QSA)
  - Validate audit scope
  - Assess PCI DSS compliance
  - Produce Report on Compliance

LBMC Security Services

LBMC INFORMATION SECURITY

What Does PCI Protect?

Protected Cardholder Data

1. The Full Contents of the Magnetic Stripe
2. The Credit Card Number
   - Also known as the PAN or Primary Account Number
3. Cardholder Name
4. The Card Security Code (aka: CVV2, CVC2 or CID)
5. The Expiration Date

PCI DSS allows the retention of certain parts of Cardholder Data, but not other parts.

LBMC INFORMATION SECURITY

PCI Data Security Standards Overview

- The PCI Data Security Standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect credit card data.
- The standard is divided into 12 requirements outlining different aspects of security best practices.
- The standard requires compliance with approximately 330 individual security validation procedures.
  - 100% compliance required to pass
  - Compensating controls can be utilized when necessary and appropriate

LBMC INFORMATION SECURITY

PCI DSS High-Level Overview

Build and 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 stored cardholder data 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 a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and 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.

LBMC INFORMATION SECURITY

Who Has to Comply With PCI DSS?

- All merchants and service providers who store, transmit, or process credit cards must comply with all requirements.
  - A merchant cannot outsource its PCI DSS responsibility
  - Merchants CAN outsource operational responsibility for maintaining security controls

- The card brands have outlined various reporting levels based on volume of card transactions.
  - Acquirer will determine a merchant's reporting level and reporting obligations
  - Merchant may have more than one acquirer (merchant ID)

LBMC INFORMATION SECURITY

How Does An Organization Prove Compliance?

That depends on the merchant/service provider reporting level…

Shown from least painful to most painful:

- Self Assessment Questionnaire (SAQ)
  - 11 different versions based on type of processing
- Results from an Approved Scanning Vendor (ASV)
- Qualified Security Assessor (QSA) Report on Compliance (RoC) and Attestation of Compliance (AoC)

LBMC INFORMATION SECURITY

Risks of Noncompliance

- Fines from card brands
  - Amount varies by card brand and is at their discretion
  - Lose ability to accept payment brand

- Breach ramifications if non-complaint
  - Penalties from payment brand
  - FTC fines and/or penalties
  - Increased legal liability (i.e., class action lawsuit)

LBMC INFORMATION SECURITY

What do I have to protect?

- PCI applies to any system that stores, processes, or transmits card data…or is connected to one of these systems.

- Effective segmentation can be use to limit the scope of PCI.

LBMC INFORMATION SECURITY

Common PCI DSS Pitfalls and Challenges

- Things that will increase the likelihood of getting hacked
- And those that will cause you to “fail your audit”

How do I avoid a compromise?

- Don't consider PCI a "check box" process
- Adequate Network Segmentation
- Know your protected data and credit card processes!
- Don't use single factor remote access
- Don't store card data if you can help it
- Proactive network monitoring
- Develop web applications securely
- Only use strong passwords to access systems
- Manage 3rd party access to systems

Common PCI Compliance Challenges

- Robust policy and process documentation (all reqs)
- Failing to consider all relevant systems in scope
- Justification for “insecure” services (FTP, telnet) (req. 1.1.5 and 2.2.2)
- Documentation of ports and protocols in/out of CDE (req.1.1.5)
- Reviewing FW rulesets biannually (not configs) (req. 1.1.6)
- Adequate secure hardening standards (industry-accepted) (req 2.2)
- Applying security patches timely (req. 6.1)
- Control and monitoring of vendor support accounts (req. 8.5.6)
- Unknowingly Storing Card Data (req 3.4)

Common PCI Compliance Challenges (con't)

- Quarterly wireless access point testing (req. 11.1)
- Obtaining "clean" quarterly vulnerability scans (req. 11.2.1)
- Retesting Penetration Test Findings
- File-integrity monitoring on all CDE components (req. 11.5)
- Third party PCI compliance monitoring (req. 12.8.4)

LBMC INFORMATION SECURITY

PCI 3.2

- PCI updates its requirements ~~every 3 years~~ (regularly).
- Starting Nov 1st everyone must be using the new requirements in version 3.2.
- Several "big impact" changes.

LBMC INFORMATION SECURITY

Multi-factor Authentication

- All admin type access must use multi-factor authentication

Service Providers Focused –

- Implement a process for the timely detection and reporting of failures of critical security control systems
- Pen test segmentation twice a year
- Quarterly confirmation of operational procedures
- Others…

SSL Clarification

- The PCI council has added an appendix making it much clearer how to address migrations to TLS 1.1 or higher and the new dates you must be off of the old technology

- (Service Providers June 30th 2016 and Merchants June 30 2018).

Merchant / Service Provider Relationship.

- You can't totally outsource PCI Compliance…
- Service Provider as part of its compliance process must identify the PCI Controls it is providing on behalf of a Merchant (and vise versa)

P2PE

LBMC INFORMATION SECURITY

Mobile Payments

Thanks! Questions & Comments

Stewart Fey, CISSP, CISA, QSA
sfey@lbmc.com
(615) 309-2479
Twitter -@Stewart_Fey

For more information:

- www.pcisecuritystandards.org
- www.lbmcsecurityservices.com

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

LBMC INFORMATION SECURITY