PCI COMPLIANCE
WHAT IS IT
AND
DOES IT APPLY TO ME?

Presented By:

Bryan Miller
CCIE, CISSP

Agenda

- Introduction
- Why the Need
- History of PCI
- Terminology
- The Current Standard
- Who Must Be Compliant and When
- What Makes this Standard Different
- Roadmap to Compliance
- So Why Care
- Product Offerings
- Final Thoughts
- Additional Information
- Questions

Introduction

- Biography
  - B.S. - Information Systems – VCU
  - M.S. – Computer Science - VCU
  - CCIE, CISSP
  - Former CCNA Instructor at John Tyler & J. Sargeant Reynolds Community Colleges
  - Current President, Syrinx Technologies LLC

Why the Need

Some famous companies in the news:

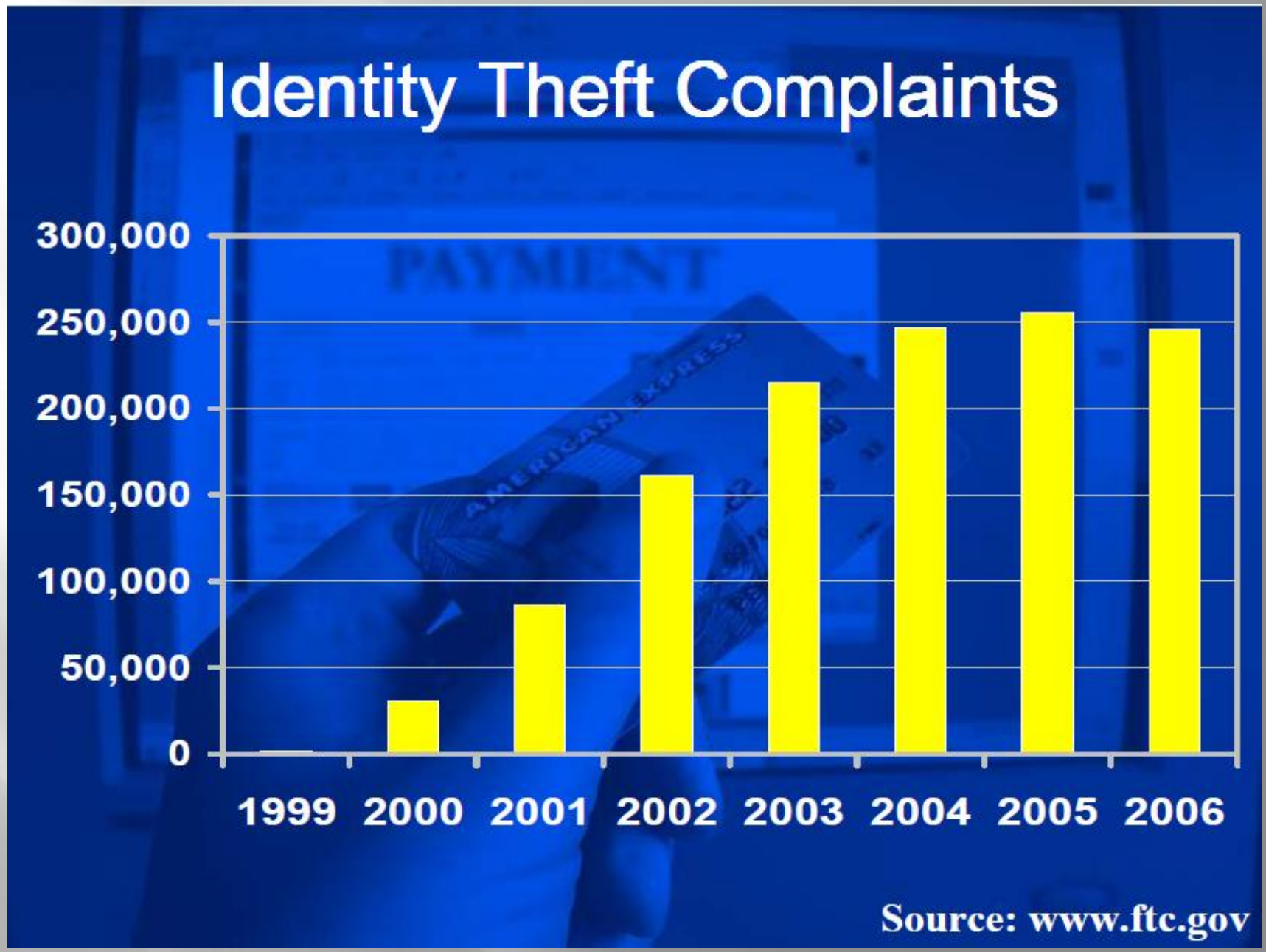
- Bank of America
- BJ's Wholesale Club
- CardSystems Solutions
- Choicepoint
- Citigroup
- DSW
- Hotels.com
- LexisNexis
- Polo Ralph Lauren
- Wachovia
- Forever 21
- Home Depot
- TJX

Top 5 Reasons for Account Data Compromise

MasterCard Worldwide

Based on MasterCard Forensics Examinations of Hacked Entities

- # Ineffective Patch Management
- # No Security Scanning
- # Weak Network Level Security
- # SQL Injection
- # Lack of Real Time Security Monitoring



History of PCI

- Sometime after 2000 the various credit card companies began thinking of ways to better protect cardholder data
- In June of 2001, VISA implemented the Cardholder Information Security Program (CISP)
- This program became known as the VISA Digital Dozen, since it had 12 areas of compliance
- In typical fashion, other credit card companies also introduced their own standards

History of PCI (2)

- In 2004, the CISP requirements were incorporated into an industry standard known as Payment Card Industry (PCI) Data Security Standard (DSS) resulting from a cooperative effort between Visa and MasterCard to create common industry security requirements

- Effective September 7, 2006, the PCI Security Standards Council (SSC) owns, maintains and distributes the PCI DSS and all its supporting documents

History of PCI (3)

- A horse by any other name:
  - American Express
    - Data Security Operating Policy
  - Discover
    - Discover Information Security & Compliance
  - JCB
    - JCB Data Security Program
  - MasterCard
    - Site Data Protection
  - VISA
    - Cardholder Information Security Plan

History of PCI (4)

- Revision History of DSS Standard
  - Published January 2005
  - Version 1.1 released Sept 7, 2006
  - Version 1.2 release October 1, 2008
- Self Assessment Questionnaire (SAQ)
  - Version 1.1 released on February 6, 2008 and became effective on April 30, 2008

Terminology

- Acquirer - Bankcard association member that initiates and maintains relationships with merchants that accept payment cards. Examples include Bank of America and WAMU.
- Approved Scanning Vendor (ASV) – Company authorized to provide quarterly scans.
- Cardholder - Customer to whom a card is issued or individual authorized to use the card
- Cardholder data - Full magnetic stripe or the PAN plus any of the following:
  - Cardholder name
  - Expiration date
  - Service Code

Terminology (2)

- Card Validation Value or Code
  - Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe.
  - The three-digit value printed to the right of the credit card number in the signature panel area on the back of the card.

- Hosting Provider - Offers various services to merchants and other service providers. Services range from shared space on a server to a whole range of "shopping cart" options.

Terminology (3)

- Magnetic Stripe Data (Track Data) - Data encoded in the magnetic stripe used for authorization during transactions when the card is presented.
- Merchant - Sell goods and maintain systems that store, process or transmit cardholder data.
- PAN - Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account.

Terminology (4)

- Qualified Security Assessor (QSA) – Company authorized to perform yearly audits.

- Service Provider - Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage or transmission of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers.

The Current Standard

- Key Point – PCI is a standard, not a regulation.
- The rule is simple, if you process, store or transmit cardholder data you must be compliant.
- 6 goals, 12 requirements

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

The Current Standard (2)

1. Build and Maintain a Secure Network

   - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data.

   - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters.

The Current Standard (2.1)

1. Build and Maintain a Secure Network

- 1.1.1 – Formal process to test and approve all changes to router and firewall configurations.
- 1.1.2 – Current network diagram with all connections to cardholder data.
- 1.1.6 – Review firewall and router rule sets every six months.
- 1.2.3 – Install perimeter firewalls between wireless networks and cardholder data networks.

The Current Standard (2.1.1)

1. Build and Maintain a Secure Network

- 2.1 – Always change vendor-supplied defaults before installing a system on the network.
- 2.2 – Develop configuration standards for all system components.
- 2.2.1 – Implement only one primary function per server.
- 2.3 – Encrypt all non-console administrative access.

The Current Standard (3)

2. Protect Cardholder Data

   - *Requirement 3:* Protect stored cardholder data.
   - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks.

The Current Standard (3.1)

2. Protect Cardholder Data

- 3.2 – Do not store sensitive authentication data even if encrypted.
- 3.2.2 – Do not store the CVV. Ever.
- 3.3 – Mask PAN when displayed (first 6/last 4).
- 3.4.1 – Disk encryption cannot be tied to local operating system accounts.

The Current Standard (3.1.1)

2. Protect Cardholder Data
   - 4.1 – Use strong cryptography and protocols such as SSL/IPSEC when transmitting data over open, public networks.
     - Internet, wireless, GSM, GPRS
   - 4.1.1 – For wireless networks, strong encryption must be used.
     - For new wireless networks, WEP is prohibited after March 31, 2009.
     - For current wireless networks, WEP is prohibited after June 30, 2010.

The Current Standard (4)

3. Maintain a Vulnerability Management Program

   - *Requirement 5:* Use and regularly update anti-virus software.

   - *Requirement 6:* Develop and maintain secure systems and applications.

The Current Standard (4.1)

3. Maintain a Vulnerability Management Program

- 5.1 – Anti-virus software must be installed on all systems affected by malicious software.
- 5.2 – Ensure that all virus signatures are current and the software is capable of generating audit logs.
- 5.2.b – The master installation of the software must be enabled for automatic updates and periodic scans.

The Current Standard (4.1.1)

3. Maintain a Vulnerability Management Program

- 6.1 – Ensure all systems have the latest vendor-supplied security patches. Install critical security patches within one month of release.
- 6.2 – Establish a process to identify newly discovered vulnerabilities.
- 6.3.2 – Separate development/test and production.

The Current Standard (4.1.2)

3. Maintain a Vulnerability Management Program

- 6.3.6 – Removal of custom application accounts, user IDs and passwords before application becomes active.
- 6.5 – Develop web apps based on secure coding guidelines such as OWASP.
- 6.6 – For public-facing web apps, one of the following:
  - Review web applications via manual or automated application vulnerability security assessment tools.
  - Install a web-application firewall in front of the web server.

The Current Standard (5)

4. Implement Strong Access Control Measures

- *Requirement 7:* Restrict access to cardholder data by business need-to-know.
- *Requirement 8:* Assign a unique ID to each person with computer access.
- *Requirement 9:* Restrict physical access to cardholder data.

The Current Standard (5.1)

4. Implement Strong Access Control Measures

- 7.1.3 – Requirement for an authorization form signed by management that specifies required privileges.
- 8.1 – Assign all users a unique ID.
- 8.3 – Use two-factor authentication for remote access to the network.
- 8.4 – Render all passwords unreadable during transmission and storage using strong cryptography.

The Current Standard (5.1.1)

4. Implement Strong Access Control Measures

- 8.5.2 – Verify user identity before performing password resets.
- 8.5.4 – Immediately revoke access for any terminated users.
- 8.5.6 – Enable accounts used by vendors for remote maintenance only during the time period needed.
- 8.5.16 – Authenticate all access to any database containing cardholder data.

The Current Standard (5.1.2)

4. Implement Strong Access Control Measures

- 9.1.1 – Use video cameras or other access control mechanisms to monitor individual physical access. Store for at least 3 months, unless otherwise restricted by law.

- 9.1.2 – Restrict physical access to publicly accessible network jacks.

The Current Standard (6)

5. Regularly Monitor and Test Networks

- *Requirement 10:* Track and monitor all access to network resources and cardholder data.

- *Requirement 11:* Regularly test security systems and processes.

The Current Standard (6.1)

5. Regularly Monitor and Test Networks

- 10.1 – Establish a process for linking all access to system components to each individual user.
- 10.2 – Implement automated audit trails for all system components.
- 10.4 – Synchronize all critical system clocks and times.
- 10.6 – Review logs for all system components at least daily.

The Current Standard (6.1.1)

5. Regularly Monitor and Test Networks

- 11.1 – Test for the presence of wireless access points at least quarterly or deploy a wireless IDS/IPS.
- 11.2 – Run internal and external network vulnerability scans at least quarterly.
  - Must be performed by an ASV.
- 11.3 – Perform external and internal penetration testing at least once a year.
  - Network and application-layer testing.
  - Internal or external resources. ASV not required.

The Current Standard (6.1.2)

5. Regularly Monitor and Test Networks

- 11.4 – Use IDS systems, and/or IPS systems to monitor all traffic in the cardholder data environment.

- 11.5 – Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files or content files. Perform file comparisons at least weekly.

The Current Standard (7)

6. Maintain an Information Security Policy

   - *Requirement 12:* Maintain a policy that addresses information security.

The Current Standard (7.1)

6. Maintain an Information Security Policy

- 12.1 – Establish, publish, maintain and disseminate a security policy.
- 12.1.3 – Includes a review at least once a year and updates when the environment changes.
- 12.3.10 – When accessing cardholder data via remote-access, prohibit copy, move and storage of cardholder data onto local hard drives and removable media.

The Current Standard (7.1.1)

6. Maintain an Information Security Policy

- 12.6 – Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.
- 12.8.2 – Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data.
- 12.9 – Implement an incident response plan. Be prepared to respond immediately to a system breach.

Who Must Be Compliant and When

Card Vendor	Merchant Level	Compliance Date
American Express	1	10/31/2006
	2	3/31/2007
	3	N/A
Discover	Use PCI DSS Levels	Use PCI DSS dates

Who Must Be Compliant and When

Card Vendor	Merchant Level	Compliance Date
MasterCard	1	6/30/2005
	2	12/31/2008
	3	6/30/2005
	4	Consult acquirer.

Who Must Be Compliant and When

Card Vendor	Merchant Level	Compliance Date
VISA	1	9/30/2004
	2	9/30/2007
	3	6/30/2005
	4	Consult acquirer.

Who Must Be Compliant and When

Card Vendor	Merchant Level	Compliance Date
PCI DSS	1	9/30/2007
	2	3/31/2008
	3	
	4	

What Makes This Standard Different

- Not a lot of ambiguity.
- Calls for specific Information Security technologies.
- The penalties are real and have been applied, up to $25K/month.
- Regularly scheduled checks to ensure continued compliancy.

Roadmap to Compliance

- Obtain upper management support
- Assign overall ownership of compliance efforts
- Develop realistic expectations
- Map data flows and identify critical devices
- Perform a gap analysis
- Select and implement security controls
- Document everything
- Understand that compliance is a process

So Why Care

- So, as a technology geek why should you care?
  - $25K/month fines could severely reduce your toys and training budget = less fun at work
  - You finally get to implement all the cool stuff you've been begging for = better resume = more money at your next job
  - It's going to make your overall network and systems more secure = fewer problems and late night pages

Product Offerings

- Lots of vendors offer products to fill one or more of the requirements
- There is no magic silver appliance
- Full compliance usually requires a combination of different vendors' products
- Some requirements can be fulfilled by open source products
- Go simple when possible

PCI Solution Mapping

PCI	ISR	ASA	CSA	MARS	WLAN	IPS	NAC	6500	Iron Port	CSM	NCM/ CAS	ACE XML	ACS
1	X	X	X	X	X	n/a	n/a	X	n/a	X	X	n/a	n/a
2	X	X	n/a	X	X	n/a	n/a	n/a	n/a	X	X	n/a	n/a
3	n/a	n/a	X	X	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
4	X	X	n/a	X	X	n/a	N/A	X	X	X	X	n/a	n/a
5	X	X	X	X	n/a	n/a	X	n/a	X	n/a	n/a	n/a	n/a
6	X	n/a	X	X	n/a	n/a	X	n/a	X	n/a	X	X	n/a
7	X	X	X	X	n/a	n/a	X	X	n/a	X	X	n/a	X
8	X	X	X	X	n/a	n/a	n/a	n/a	n/a	X	X	n/a	X
9	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
10	X	X	X	X	X	X	n/a	X	n/a	X	X	n/a	X
11	X	X	X	X	X	X	n/a	X	n/a	X	X	n/a	n/a
12	X	X	X	X	X	X	X	X	X	X	X	X	X

Final Thoughts

- PCI Compliance != Enterprise Security
  - Best Western – 8-13 million credit cards
  - Hannaford Groceries – 4.2 million credit cards
    - 2 lawsuits
  - Forever 21 – 98,000 credit cards

- Texas HB 3222 – Banks and credit unions can recoup costs for re-issuing credit cards if merchant isn't PCI compliant. Other states will inevitably follow.

Additional Information

- PCI Security Standards
- American Express Data Security
- Discover Information Security & Compliance
- JCB Global Site
- MasterCard Site Data Protection Program
- VISA Cardholder Information Security Program (CISP)

Additional Information (2)

- Cisco PCI Information
- Juniper PCI Information
- Qualsys
- F5 Labs
- Syrinx Technologies

Questions

Thank You Very Much for Your Time and Attention!