Colorado
Mountain
College

PCI Compliance

What is it?
Who uses it?
Why is it important?

Definitions:

- PCI- Payment Card Industry
- DSS-Data Security Standard
- Merchants—Anyone who takes a credit card payment
- 3rd party processors—companies like Paypal

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that [redacted]. companies that [redacted], [redacted] or [redacted] credit card information maintain a secure environment

- Any merchant that has a Merchant ID (MID).

Is it Secret, is it Safe?

PCI-DSS Requirements

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

PCI-DSS Requirements

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access

PCI-DSS Requirements

- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

FAQs

- Applies to?
  - All organization or merchants regardless of size
  - Payments over the phone (only)
  - Even if you use 3rd party processors
  - Debit as well as credit cards

FAQs

- What is cardholder data
  - Any personally identifiable data associated with cardholder
  - These include: acct #, expiration date, name, address, social security #

Myths

- “I’m a small merchant who only takes a handful of cards, so I don’t need PCI
  - Even if only one or two still need to be compliant
- Out-sourcing card processing makes us compliant
  - Simplifies but not provide automatic compliance. Should request a certificate of compliance annually from providers

Myths

- PCI compliance is an IT project
  - They may implement it, but it's an on-going process that involves everyone
- PCI is unreasonable and is too hard
  - Most aspects are already common sense best practices for security.

BREACHES

- Also known as a cardholder Data compromise
- An unauthorized individual taking advantage of a flaw in the system

Breaches

- An event in which an individual's name plus any or all of these:
  - Social Security Number (SSN),
  - Driver's license number,
  - Medical record
  - Financial record/credit/debit card
    - is potentially put at risk –
    - either in electronic or **paper** format

Who is at risk

- Food service and retail 77%
- Smaller merchants 85%
- Card present 69%
- Card not present 31%
- Universities 3%

Security Incidents

- Celebrity hospital records accessed and then leaked—

- An employee left back-up tapes on a desk rather than physically handing the tapes off to the courier and they were stolen

- 2006, a U.S. Department of Affairs employee took a laptop home for work purposes; subsequently, the laptop was stolen, exposing personal data of over 26.5 million veterans

University Breaches

- At least 50 have been breached more than once since 2001
  - Purdue University (7 times)
  - University of Florida (5 times)
  - Ohio State University (4 times)
- Most of these were social security numbers and other personal information, some included credit card numbers

University Breaches

- Three main causes of breaches at the University level
  - Unauthorized access (usually inside jobs)
  - Accidental on-line exposures
  - Stolen laptops
- Highest months are Jan and May
  - Registration months for most schools

Threats

- Can come from outside the network (hackers, competitors, etc)
- Can also come from within
  - Disgruntled employees
  - Vendors or guests can knowingly or unknowingly compromise a network

Insider Threats

- A well-meaning Employee
  - ➢Unintentionally breaks security policy or exposes sensitive information through social networks, blogs or insecure Wi-Fi
  - ➢Loss or theft of a laptop or portable storage device
  - ➢Phishing attacks
  - ➢Ignoring or circumventing security policy to meet a business need

Insider Threats

- Malicious Employees
  - ➢Intentionally breaks security policy
  - ➢Uses the corporate network for unacceptable activity
  - ➢Steal or sabotage corporate data

Insider Threats

- Well-meaning employees become "accidental" threats when:
  - ➢They are not aware of the security threats to their organization
  - ➢They are relying on someone else to deal with security threats
  - ➢They are not adequately equipped to address these threats
  - ➢They may feel there are more important things to focus on

Insider Threats

- Other inherent issues for businesses:
  - ➢No feeling of personal responsibility for security
  - ➢Security awareness education not seen as a high priority
  - ➢Budgets and staff may be limited for security

Risky behaviors by businesses

- 81% store payment card numbers
- 73% store payment card exp dates
- 71% store payment card verification codes
- 57% store customer data from the payment card magnetic strip
- 16% store other personal data

- Protect both electronic data and paper receipts

Non-compliance: Risks, Fines, Fees, Costs, Loss

- Non-compliant, compromised business could expect the following:
  - ❑Damage to brand/reputation
  - ❑Investigation costs
  - ❑Remediation costs
  - ❑Re-issuance
  - ❑Fraud loss
  - ❑Ongoing compliance audits
  - ❑Victim notification costs

Non-compliance: Risks, Fines, Fees, Costs, Loss

- Non-compliant, compromised business could expect the following:
  - ❑Financial loss
  - ❑Data loss
  - ❑Charge-backs for fraudulent transactions
  - ❑Operations disruption
  - ❑Sensitive information disclosure
  - ❑Denial of service to customers
  - ❑Individual executives held liable
  - ❑Possibility of business closure

Data Do's

- Use Cryptography to protect data
- Understand the entire process and where the card information travels electronically
- Make sure that your payment applications meet PCI compliance standards
- Store cardholder data only if you have a valid business need to save this info
- Make sure the data is secured in a protected environment

Data Do's

- Make certain that 3rd parties who process your credit card payments understand and comply with all PCI DSS standards
- Give each administrator a unique password and ID

Data Dont's

- Store card holder data in an unsecure device, such as laptops or cell phones
- Have the PIN entry device print out personal cardholder information
- Keep authentication data stored on the customer's payment card chip or magnetic strip
- Store the validation code after authorization

Data Don’ts

- Store cardholder data unless you have a justifiable business need for doing so
- Allow anyone except authorized personnel to access stored card holder data
- Use payment card system storage devices that are not stored in a locked and protected access room

Physical Security

- Where is it located
  - On a computer hard drive
  - On computer media (CDs, DVDs, backup tapes, etc.)
  - On paper

- All of the above can be taken by someone outside your business

Physical Security

- Questions
  - Where do you store your computers, media and paper records with cardholder data on it?
    - Are those locations locked?
    - Who has access to them?
  - Do those same resources ever leave the premises?
    - How do you track those resources in transit?
    - Where do they end up?
  - Do you monitor access to those resources?

Best Practices

- Training should include
  - Industry rules/regulations
  - Specific responsibilities
  - Proper handling of sensitive data
  - Proper protection of sensitive information
  - Proper methods for handling physical/sensitive information

Best Practices

- People/Process/Technology
  - What does company consider appropriate behavior
  - Incorporate these into daily business
  - Have an effective accountability mechanism

Fundamental Best Security Practices

- Avoids fraud
- Upholds Brand Name
  - Adds value to name
  - Increases consumer confidence
  - Improves reputation
  - Clarifies where data is stored
  - Helps to understand own system better

Best Practices

- Training should emphasize
  - ➢Industry rules and regulations
  - ➢Responsibilities of managers and employees
  - ➢Proper handling of sensitive data, such as cardholder data and proprietary company data
  - ➢Proper protection of sensitive information, including password protection
  - ➢Proper methods for handling sensitive material, such as during transmission, storage and destruction

Before starting a program

- Gather input from within organization to determine priorities
- Support your program with strong, clear policies
  - Employees need to know what actions they are responsible for and why
- Identify specific roles within your organization
  - Cashiers have different responsibilities than data center staff

Resources and References

- Your own IT department
- PCI websites:
  - http://www.pcicomplianceguide.org/
  - http://www.pcifree.com/
  - http://www.pciknowledgebase.com/
- Your own bank website
- Your own credit card processor website
- Trustwave www.trustwave.com
- Minnesota Privacy Consultants and Jay Cline of Computer World magazine