PCI DSS Training

Brent Hobby, CISM, CISA, QSA
Security Advisor
CampusGuard

Ivy Rasmussen, PCIP
Customer Relationship Manager
CampusGuard
Agenda

- Introductions
- PCI Overview
- Common PCI Myths
- Compliance and Validation
- Managing Scope
- Data Breaches
- Managing Compliance
- What’s New and What to Watch
- Q&A
CampusGuard

- 10th anniversary year
- International Information security, privacy, and compliance firm
- Qualified Security Assessor (QSA)
- Approved Scanning Vendor (ASV)
- Perform compliance and security assessments, vulnerability scans, penetration tests, on-going support, and training
- Focused on campus-based organizations including Higher Education, Healthcare, and State & Local Government
CampusGuard Services

- Assessments
- Offensive Security Services
- Annual Support
- Training

Information Security
- Program Evaluation
- Vulnerability Testing
- Penetration/Segmentation Testing
- Web Application Testing
- Social Engineering
- Incident Response Plan Testing
- Policy and Procedure Review

Compliance
- PCI DSS
- GLBA
- NACHA/ACH
- HIPAA and HITECH
- GDPR
- FERPA
- FACTA/Red Flags
CampusGuard Service Delivery

Customer Relationship Manager
Ivy Rasmussen, PCIP

Security Advisor
Brent Hobby, QSA, CISA, CISM

CampusGuard Family
Everybody!
Agenda

- Introductions
- PCI Overview
- Common PCI Myths
- Compliance and Validation
- Managing Scope
- Data Breaches
- Managing Compliance
- What’s New and What to Watch
- Q&A
PCI Overview

- **PCI-DSS**
  - Payment Card Industry Data Security Standard

- Common set of card data security measures.

- Every merchant is responsible for safeguarding cardholder data, can be held liable for security compromises, and is **contractually obligated** to comply with PCI-DSS.
PCI Overview

PCI DSS: “One Standard to Rule Them All”

- Cardholder Information Security Program (CISP)
- Data Security Standard (DSS)
- Data Security Operating Policy
- Information and Compliance
- Site Data Protection (SDP)
- Data Security Program
PCI DSS Framework
6 Goals with 12 Requirements

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
Who Must Comply?

Do you....

- Store, process, or transmit cardholder data?
  - Point-of-Sale (POS)
  - Mail Order / Telephone Order (MOTO)
  - Fax
  - E-Commerce / Website
- Own the merchant account (MID) that takes payments?
- Have the ability to affect the security of cardholder data?

IF YOU ANSWER YES TO ANY OF THE ABOVE QUESTIONS THEN PCI DSS APPLIES TO YOU!
Players in the Payment Lifecycle

Issuer

Acquirer

Cardholder

Merchant

Service Providers
PCI Relationships

**Acquirer**
Communicates and educates merchants on PCI DSS and reports compliance status to card brands

**Merchant**
Responsible for safeguarding credit card data and complying with the PCI DSS

**CREDIT CARD SECURITY**

Responsible for managing the PCI DSS and certifying QSAs and ASVs

Responsible for enforcing and monitoring merchant compliance with the PCI DSS
How is PCI Enforced?

Merchants have contracts with Service Providers requiring them to protect cardholder data.

The brands have contracts with banks requiring them to ensure their merchants are PCI compliant.

The banks have contracts with merchants requiring them to be PCI compliant.

Unlike regulations, PCI DSS is enforce by contract.
PCI’s Multiple Standards

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data

- Manufacturers
  - PCI PTS
    - PIN Entry Devices
- Software Developers
  - PCI PA-DSS
    - Payment Applications
- Merchants & Service Providers
  - PCI DSS
    - Secure Environments
- P2PE

Ecosystem of payment devices, applications, infrastructure and users
Covered Data Elements

What’s PCI Trying to Protect?
# Covered Data Elements

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder name</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Service code</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Expiration date</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Sensitive Authentication Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Magnetic stripe/Track equivalent (chip)</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
<tr>
<td>CVC2/CVV2/CID</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
<tr>
<td>PIN/PIN block</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
</tbody>
</table>
## Merchant Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Criteria</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| 1     | • More than six million Visa/MasterCard/Discover transactions annually (2.5 million American Express)  
• Any merchant that has suffered a Cardholder Data compromise | • Annual Onsite PCI Data Security Assessment (ROC)  
• Quarterly ASV scans |
| 2     | • One-to-Six million transactions annually (50,000 American Express) | • ROC or QSA assisted SAQ  
• Quarterly ASV scans |
| 3     | • 20,000-to-One million e-commerce transactions annually | • Annual SAQ  
• Quarterly ASV scans |
| 4*    | • Less than 20,000 e-commerce transactions or up to 1 million transactions annually  
* n/a American Express | • Annual SAQ*  
• Quarterly ASV scans*  
* Acquirer discretion |
Payment Methods

■ Card-Present
  ■ Point-of-Interaction Device (POI)

■ Card-Not-Present
  ■ E-commerce (web/mobile)
  ■ Mail
  ■ Telephone
  ■ Fax

“MOTO Transactions”
## Payment Methods

<table>
<thead>
<tr>
<th>SAQ</th>
<th>Count</th>
<th>Payment Method</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>24</td>
<td>Card-not-present merchants; all cardholder data functions fully outsourced to validated third parties</td>
<td>Green</td>
</tr>
<tr>
<td>P2PE</td>
<td>34</td>
<td>PCI Council listed P2PE solutions, only terminals approved for the solution No electronic CHD storage</td>
<td>Green</td>
</tr>
<tr>
<td>B</td>
<td>41</td>
<td>Merchants with only imprint machines or only standalone, dial-out terminals No electronic cardholder data storage</td>
<td>Green</td>
</tr>
<tr>
<td>C-VT</td>
<td>84</td>
<td>Merchants with web-based virtual terminals hosted by validated third parties No electronic CHD storage</td>
<td>Yellow</td>
</tr>
<tr>
<td>B-IP</td>
<td>87</td>
<td>Merchants with standalone, IP-connected PTS-approved Point-of-Interaction (POI) terminals – No electronic CHD storage</td>
<td>Yellow</td>
</tr>
<tr>
<td>C</td>
<td>161</td>
<td>Merchants with payment application systems connected to the Internet No electronic CHD storage</td>
<td>Red</td>
</tr>
<tr>
<td>A-EP</td>
<td>192</td>
<td>Partially outsourced ecommerce merchants using validated third party websites for payment processing</td>
<td>Red</td>
</tr>
<tr>
<td>D</td>
<td>328</td>
<td>All other SAQ-eligible merchants</td>
<td></td>
</tr>
<tr>
<td>D-SP</td>
<td>370</td>
<td>All SAQ-eligible service providers</td>
<td></td>
</tr>
</tbody>
</table>

Confidential Property of CampusGuard
Let’s Review

What does PCI-DSS stand for?

1. Protect Computer Industry - Data Security Standard
2. Payment Card Industry - Data Security Standard
3. Payment Card Industry - Data Safety Standard
4. Payment Card Identification - Develop Security Service

(2) Payment Card Industry Data Security Standard
Let’s Review

PCI DSS applies to you if:

1. You accept mobile payments
2. You accept payment cards
3. You accept payments online
4. You use a third-party to process payments

(2) PCI DSS applies if you store, process, transmit, or can affect the security of cardholder data.
Agenda

- Introductions
- PCI Overview
- Common PCI Myths
- Compliance and Validation
- Managing Scope
- Data Breaches
- Managing Compliance
- What’s New and What to Watch
- Q&A
Common PCI DSS Myths

- “I can wait until the bank asks me to be compliant.”
- “Since the bank hasn’t asked me, I don’t have to be compliant.”

All merchants needed to be compliant with the PCI DSS by June 2005 (Sept 2006 for v1.1)
Common PCI DSS Myths

- “I don’t store credit card numbers, so I have no compliance obligation with the PCI DSS.”
- “I only process a few credit card transactions per year, so I am exempt from compliance with the PCI DSS.”

The PCI DSS globally applies to all entities that store, process or transmit cardholder data.
Common PCI DSS Myths

“I only need to be mostly compliant with the PCI DSS.”

The PCI DSS is pass/fail. To be considered compliant, you must answer affirmatively for all requirements.
Agenda

- Introductions
- PCI Overview
- Common PCI Myths
- Compliance and Validation
- Managing Scope
- Data Breaches
- Managing Compliance
- What’s New and What to Watch
- Q&A
Compliance and Validation

- While everyone must be compliant, most* must also validate compliance via assessment.
- Different levels of Merchants may require third party validation (ROC - QSA).
- Others will require the SAQ.
  - Requires executive level signoff.
  - Be sure you are compliant before signing!
- May require quarterly scanning.

* Validation for level 4 merchants is at the discretion of the acquiring bank, depending on the card brand.
Newer PCI Requirements

- Data flow diagram now required (1.1.3)
- Inventory of all components (2.4)
- Protect points of physical interaction from tampering and substitution (9.9)
- Include verification of PCI DSS requirements on change control processes (6.4.6)
- Incorporate multi-factor authentication (MFA) for administrative access into the CDE (8.3.1)
- Maintain information about which PCI DSS requirements are managed by each service provider (12.8.5)
- Service providers must provide written acknowledgement (12.9)
Securing Points of Interaction

- Requirement 9.9 took effect **July 1, 2015**.
  - Maintain an inventory list of devices
  - Periodically inspect devices for tampering or substitution
  - Train personnel to be aware of and report suspicious behavior.

**Information Supplement**

*Skimming Prevention: Best Practices for Merchants*

*Version 2.0*
Requirement 9.9 - Skimmer
Teamwork: Skimmer Installation
EMV: Europay, MasterCard, Visa

- “Chip” Cards
- EMV is a separate standard
- Supports PCI DSS in a layered security approach
- Protects against card fraud
- Affects only physical points of interaction
- Pushes fraud to other payment channels
Let’s Review

You cannot store data in electronic or paper format.

1. True
2. False
3. Both

(3) Trick Question 😊 While it’s technically possible to store cardholder data (CHD) in compliance with PCI DSS requirements, IT IS AGAINST UNIVERSITY POLICY TO STORE CHD.
Let’s Review

How long have merchants been required to be compliant with the PCI DSS?

1. September, 2003
2. September, 2004
3. September, 2006
4. September, 2008

(3) PCI DSS Version 1.1 was released on September 7th, 2006
Agenda

- Introductions
- PCI Overview
- Common PCI Myths
- Compliance and Validation
- Managing Scope
- Data Breaches
- Managing Compliance
- What’s New and What to Watch
- Q&A
Defining Your PCI DSS Scope

- **Merchant**
  - Accepts payment cards
  - Owns a Merchant ID (MID)

- **Service Provider**
  - Stores, processes, or transmit CHD on behalf of another entity
  - Provides services that control or could impact the security of CHD
    - Exception – Internet Service Providers (ISP)
Defining Your PCI DSS Scope

- People, processes, and technologies that store, process, or transmit cardholder data, or that could affect the security of cardholder data.

- Any systems that reside in or connect to the Cardholder Data Environment (CDE).
What’s in PCI Scope?

- Card Swipe Machine?
- Office Workstations?
- Student?
- Shopping Cart?
- Computer Lab?
- Phone Transaction?
Outside Payment Processing

- Using a 3rd party to process payments for the institution may alleviate some scope and PCI DSS requirement considerations:
  - Event registrations, day camps, T-shirt sales etc.
  - Sites that contain a “Pay Now” button that redirects or uses embedded code to a 3rd party.
- Processing transactions *FOR* a 3rd party can make the institution a PCI service provider

You can never outsource your ultimate PCI compliance responsibility
Scope Creep

What happens when employees enter data for the customer on their machines?

- The DSS is definitive about CHD transmission
- This no longer fits the definition of “E-Commerce”
- The employees’ workstations come into scope
- If not segmented…
  the general network also comes into scope.
PCI DSS Scope and Risk

- Scope = Risk
- Increased Scope = Increased Risk
- Increased Risk = Increased Cost

- Risk and Cost roughly track SAQ complexity and number of compliance questions

You can never outsource your ultimate PCI compliance responsibility
## Merchant Risk and Complexity

<table>
<thead>
<tr>
<th>SAQ</th>
<th>Count</th>
<th>Payment Method</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>24</td>
<td>Card-not-present merchants; all cardholder data functions fully outsourced to validated third parties</td>
<td>Green</td>
</tr>
<tr>
<td>P2PE</td>
<td>34</td>
<td>PCI Council listed P2PE solutions, only terminals approved for the solution No electronic CHD storage</td>
<td>Green</td>
</tr>
<tr>
<td>B</td>
<td>41</td>
<td>Merchants with only imprint machines or only standalone, dial-out terminals No electronic cardholder data storage</td>
<td>Yellow</td>
</tr>
<tr>
<td>C-VT</td>
<td>84</td>
<td>Merchants with web-based virtual terminals hosted by validated third parties No electronic CHD storage</td>
<td>Yellow</td>
</tr>
<tr>
<td>B-IP</td>
<td>87</td>
<td>Merchants with standalone, IP-connected PTS-approved Point-of-Interaction (POI) terminals – No electronic CHD storage</td>
<td>Yellow</td>
</tr>
<tr>
<td>C</td>
<td>161</td>
<td>Merchants with payment application systems connected to the Internet No electronic CHD storage</td>
<td>Red</td>
</tr>
<tr>
<td>A-EPI</td>
<td>192</td>
<td>Partially outsourced ecommerce merchants using validated third party websites for payment processing</td>
<td>Red</td>
</tr>
<tr>
<td>D</td>
<td>328</td>
<td>All other SAQ-eligible merchants</td>
<td>Red</td>
</tr>
<tr>
<td>D-SP</td>
<td>370</td>
<td>All SAQ-eligible service providers</td>
<td>Red</td>
</tr>
</tbody>
</table>
Segmentation

Segment the CDE

- Only payment and connected systems are in scope
Point-to-Point Encryption: P2PE

Simplifies compliance with PCI DSS

- Cardholder data (CHD) is encrypted by the hardware at the point of interaction (POI)
- Decryption of CHD happens outside of the merchant environment
- Merchant’s infrastructure is out of scope for PCI attestation.
Point-to-Point Encryption: P2PE

- Secure encryption of payment card data at the POI
- P2PE validated application(s) at the POI
- Secure device management
- Secure management of decryption
- Use of secure encryption technology and methodologies

Follow the PIM (P2PE Instruction Manual)
SAQ A

- FOR: Card-not-present merchants
  - E-commerce or mail/telephone order

- NOT FOR: Face-to-face channels

- For merchants that have outsourced payment card processing to a third-party PCI-compliant service provider
  - Website fully hosted and managed
  - Website provides an inline frame (iframe) or full redirection
  - No storage, processing, or transmission of cardholder data (CHD) on your systems or premises.
SAQ B

- FOR: In-person or mail/telephone (MOTO) order merchants

- NOT FOR: E-commerce channels

For merchants that use standalone dial-out terminals
  - Terminals only connected to phone line
  - Also applies to imprint machines (a.k.a. knuckle busters)
  - No electronic storage of cardholder data
SAQ C

- **FOR:** In-person or mail/telephone (MOTO) order merchants

- **NOT FOR:** E-commerce channels

- For merchants that have a *payment application* and an Internet connection on the same device or network
  - Payment application is not connected to other systems
  - Applies only to single locations
  - No electronic storage of cardholder data
SAQ P2PE (Point-to-Point Encryption)

- FOR: In-person or mail/telephone (MOTO) order merchants
- NOT FOR: E-commerce channels
- For merchants using a listed PCI-validated P2PE solution
  - Solution must follow the P2PE Instruction Manual (PIM)
  - No electronic cardholder data storage.
Agenda

- Introductions
- PCI Overview
- Common PCI Myths
- Compliance and Validation
- Managing Scope
- Data Breaches
- Managing Compliance
- What’s New and What to Watch
- Q&A
DBIR: Trends

- Shift from ATM/POS skimming towards e-commerce applications
- Breaches compromising payment cards are increasingly about web servers
DBIR: Compromise Detection

It’s time to act.

Most compromises took minutes, or less

Compromise

87%

Only 3% are discovered as quickly

Two-thirds went undiscovered for months or more

68%

Elapsed time

< Before the compromise

After the compromise >

Months

Weeks

Days

Hours

Minutes

Hours

Days

Weeks

Months

Confidential Property of CampusGuard
DBIR: Attack vs. React

Figure 28. Breach timelines
Cost of a Data Breach

In the event of a data breach, the card brands can:

- Assess fines
  - Up to $500,000 per brand per breach
- Require that you notify victims
- Require that you pay card replacement costs
- Require that you reimburse fraudulent transactions
- Require forensic investigations be performed by a PCI approved firm
- Require that you validate as a Level 1 merchant (QSA)

*** Merchant Risk is Always the University’s ***
Third-Party Breaches

- Almost 60% of companies experience a data breach caused by a third party
  - Of the 54 major breaches disclosed in 2018, the top three involved third parties:
    - 11 Cloud-based storage, service, or hosting provider
    - 9 Online Payment, credit card processing, or point-of-sale system
    - 7 JavaScript Library

- 22% of those surveyed do not know if they’ve had a 3rd party breach
- Only one-third have an inventory of vendors with whom they share sensitive data
- Third-party involvement, which increases the cost by roughly 10%.

- Data Risk in the Third Party Ecosystem, 2018, Ponemon Institute
Consequences

Direct Costs
- Discovery / Forensics
- Notification costs
- Identity monitoring costs
- Additional security measures
- Lawsuits
- Fines

Indirect Costs
- Loss of customer confidence
- Loss of productivity
- Distraction from core business
- Level 1 merchant classification

10,000 accounts X ~$233 / account = $2.33 Million

Reputation – Priceless!

1 “2019 Cost of a Data Breach” (Ponemon Institute)
Let’s Review

I don’t store credit card numbers, so I have no official compliance obligation with the PCI DSS.

1. True
2. False

(2) The PCI DSS globally applies to all entities that store, process or transmit cardholder data; not just those that store data.
Let’s Review

Merchants can process payment card transactions on any University owned and managed workstation.

1. True
2. False

(2) Using general purpose workstations for payment card processing will usually bring the University’s entire network resources into PCI scope. Merchants should restrict payment card activities to specifically designated systems.
Agenda

- Introductions
- PCI Overview
- Common PCI Myths
- Compliance and Validation
- Managing Scope
- Data Breaches
- Managing Compliance
- What’s New and What to Watch
- Q&A
A Campus is a “City”

Challenges for PCI Compliance:
- Open networks and systems
- Scope creep
- Overloaded staff
- Fiscal constraints
PCI Compliance

- Compliance with PCI DSS is a continuous process that begins with an **assessment** of the environment.

- **Remediation** is the process of addressing vulnerabilities.

- Regular **reports** are required to validate PCI DSS compliance.
PCI Compliance Process

Discovery and Assessment → Remediation → Validation → Remediation

- Payments Analysis
- Merchant Discovery
- Documentation
- Preliminary Scanning
- Gap Analysis

- Correct Problems
- Compensating Controls
- ROC or SAQ Submission
- Quarterly Scanning
- Penetration Testing

Re-Validate every 12 months
Some Best Practices

- NEVER email credit card information
- NEVER store credit card numbers in any database or spreadsheet
- Keep credit card documentation locked in a safe or SECURE filing cabinet
- Destroy documentation containing credit card information when no longer needed for business or legal reasons
- Permit only those employees who have a legitimate “need-to-know” access to cardholder info
# PCI DSS Framework

6 Goals with 12 Requirements

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

Build and Maintain a Secure Network

- Requirement 1: Firewall installation and network configuration
  - 27 Questions
    - Restrict inbound and outbound traffic to that which is necessary
    - Implement stateful packet inspection
    - Review rule sets every six months

- Requirement 2: Eliminate vendor default credentials and system hardening
  - 29 Questions
    - Encrypt all non-console administrative access
    - Remove all unnecessary functionality – scripts, drivers, features, etc.
Objective 2
Protect Cardholder Data

Requirement 3: Protect stored cardholder data

- 31 Questions
  - Limit storage of cardholder data; develop retention policies
  - Render all stored data readable: encryption, masking, etc.
  - Use strong cryptography

Requirement 4: Encrypt transmission of cardholder data

- 9 Questions
  - Use strong cryptography when transmitting across open networks
  - Wireless network specifically
  - Never transmit PAN through email, chat, or other insecure means
Objective 3
Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update antivirus software
  - 8 Questions all relating to antivirus, updates, scans, and logging

- Requirement 6: Develop and maintain secure systems and applications
  - 34 Questions
    - Latest patches
    - Secure coding
    - Separation between development and production
    - Change control
    - Web application code review **OR** Web application firewall
Objective 4
Strong Access Control

- Requirement 7: Restrict Access – Need to know
  - 9 Questions
    - Limit access to systems to those with business need
    - Role based privilege
    - Automated access control

- Requirement 8: Assign unique IDs and control authentication
  - 29 Questions
    - Incorporate multifactor authentication for remote access
    - Render password passwords unreadable during transmission
    - Enable vendor accounts only when needed
    - Minimum password length and change parameters

- Requirement 9: Restrict physical access to CHD
  - 43 Questions
    - Facility entry controls and access
    - Backup storage; Shred, incinerate, pulp, paper storage
Objective 5
Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and CHD
  - 37 Questions
    - Implement automated auditing of all CHD access
    - File-integrity monitoring and protection of stored logs
    - Log retention and review

- Requirement 11: Regularly test security systems and processes
  - 32 Questions
    - Quarterly testing for rogue wireless
    - Internal and external vulnerability assessments
    - Application layer and network penetration testing
    - IDS/IS
    - File-integrity monitoring
Objective 6
Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

- 46 Questions
  - All points of the PCI DSS
  - Risk assessment
  - Critical technologies
  - Security roles
  - Education and verifications
  - Background checks
  - 3rd Party associations
  - Incident response
PCI DSS Clarifications

- Wireless is only in scope if it is used for storing, processing, or transmitting CHD
- With proper segmentation the “untrusted” network can be part of the “corporate” LAN
- Storage – committed to disk/NVRAM
Summary of the twelve requirements of the PCI DSS

1. Install/maintain a firewall
2. No default credentials/settings
3. Protect stored CHD
4. Encrypt transmitted CHD
5. Use/update antivirus software
6. Develop/maintain secure systems and applications
7. Restrict access, need-to-know
8. Assign unique user IDs
9. Restrict physical access to CHD
10. Track/monitor access to resources and CHD
11. Test systems and processes
12. Maintain an information security policy
Let’s Review

You can send or receive cardholder data via email as long as the email is deleted afterward?

1. True
2. False

(2) Never send or receive cardholder information via email. Payment card numbers must not be transmitted in an insecure manner, such as email, unsecured fax, or through campus mail.
Let’s Review

What steps should a merchant take if they suspect cardholder data has been compromised?

1. Immediately contact the cardholder
2. Go to lunch
3. Review the Incident Response Plan
4. Ignore it. It will probably be OK.

(3) All incidents must be immediately reported following the process documented in the Incident Response Plan.
Agenda

- Introductions
- PCI Overview
- Common PCI Myths
- Compliance and Validation
- Managing Scope
- Data Breaches
- Managing Compliance
- What’s New and What to Watch
- Q&A
What’s New and What to Watch

- Pre-Authorized Returns and PIN Prompting
- P2PE Growth
- Biometrics/Identity
  - Visa and Mastercard have both introduced fingerprint cards
  - Ticketless transportation?
- Contactless Payments (NFC) / Mobile Wallets
  - 50% of payments will be mobile in 2020
- Person-to-Person Transactions
- Artificial Intelligence
- Blockchain for reconciliation and accounting
- PCI-DSS 4.0
PCI DSS Development

Goals for PCI DSS v4.0

- Ensure the standard continues to meet the security needs of the payments industry
- Add flexibility and support additional methodologies to achieve security
- Promote security as a continuous process
- Enhance validation methods and procedures
PCI DSS Development

What are they looking at?

- Authentication
  - Multi-Factor Authentication
  - NIST Password Guidance
- Broader applicability for encrypting cardholder data
  - Specifically on trusted networks
- Greater consideration of technology advancement
- Greater frequency of testing critical controls
  - Continuous Oversight / Information Assurance
- Redirected Payments (SAQ A)
Resources

- PCI Security Standards Council
  - www.pcisecuritystandards.org
- Card Brands
  - www.visa.com/cisp
  - www.mastercard.com/sdp
- Privacy Rights Clearinghouse
  - www.privacyrights.org
- KrebsOnSecurity
  - www.krebsonsecurity.com
- Ponemon Institute
  - www.ponemon.org
- CampusGuard
  - www.campusguard.com
Brent Hobby, CISM, CISA, QSA
Security Advisor
CampusGuard
bhobby@campusguard.com