Northwestern

PCI DSS Training

Pete Campbell, CISA, QSA
Security Advisor
CampusGuard

Confidential Property of CampusGuard

Introducing CampusGuard

CAMPUSGUARD®

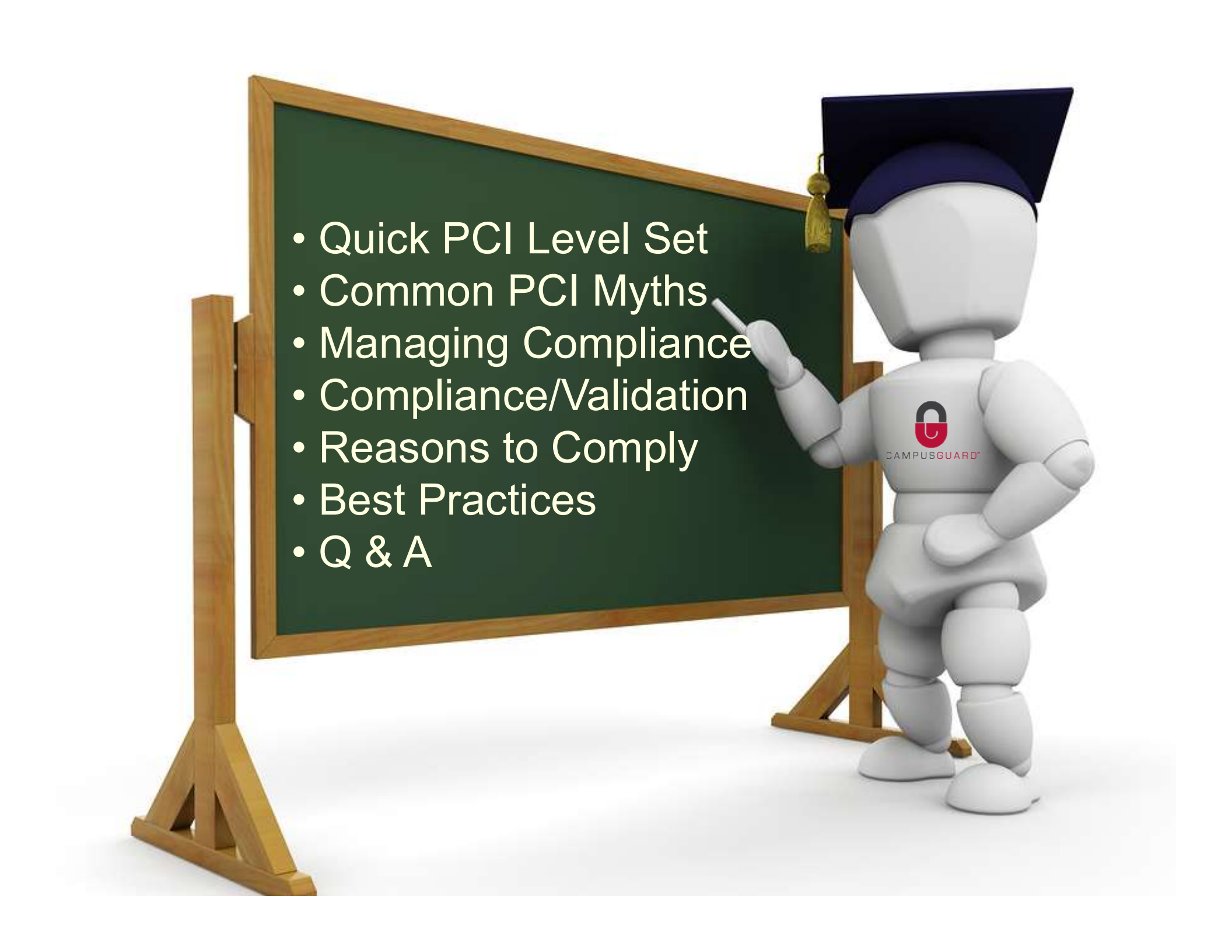
A Merchant Preservation Services Company

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council™
APPROVED SCANNING VENDOR

- **Full service QSA/ASV firm for PCI DSS compliance**
- **Certified in US, Australia and New Zealand**
- **Focused primarily on campus environments**
- **We understand the PCI DSS and how it applies to diverse merchant environments**

Confidential Property of CampusGuard

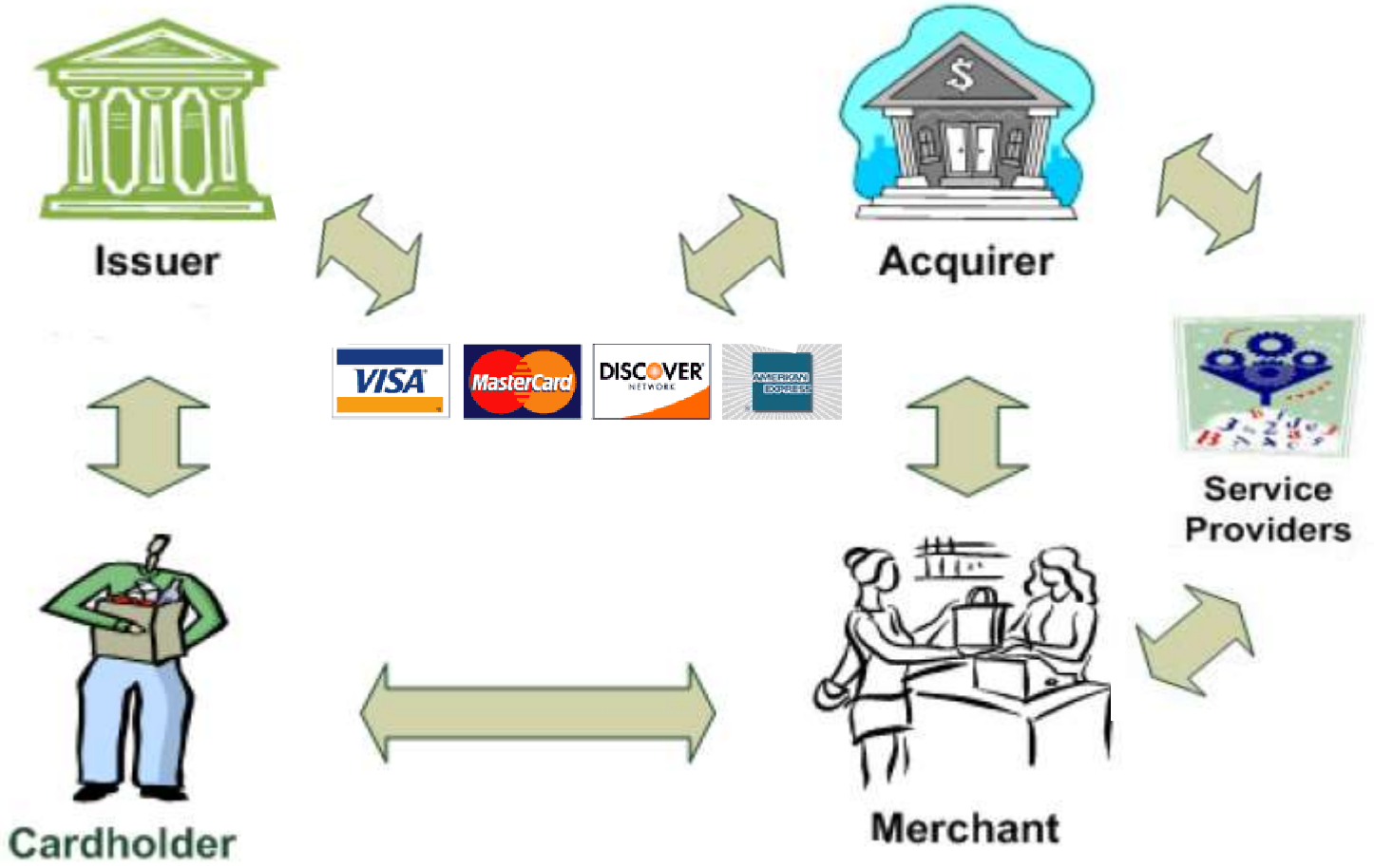

• Quick PCI Level Set
• Common PCI Myths
• Managing Compliance
• Compliance/Validation
• Reasons to Comply
• Best Practices
• Q & A
CAMPUSGUARD

Payment Card Industry Data Security Standard (PCI DSS)



Confidential Property of CampusGuard

Players in the Payment Lifecycle



Confidential Property of CampusGuard

PCI Relationships



Responsible for managing the PCI DSS and certifying QSAs and ASVs

Acquirer

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

CREDIT CARD SECURITY



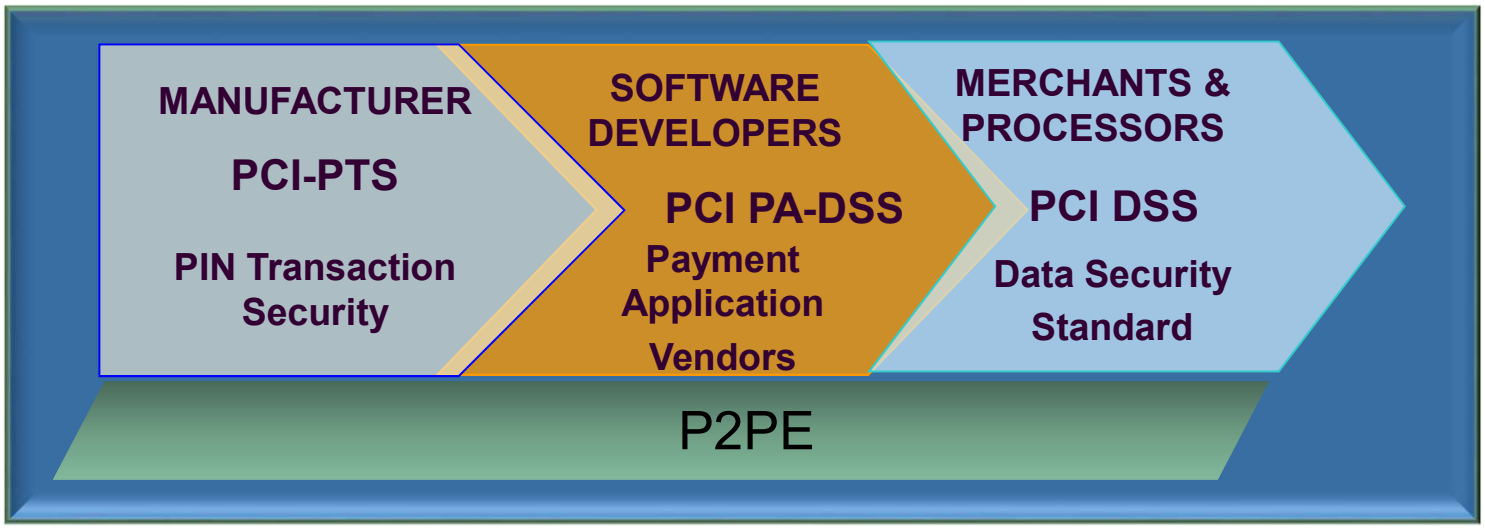
Responsible for enforcing and monitoring merchant compliance with the PCI DSS

Merchant

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

Confidential Property of CampusGuard

PCI = Multiple Standards



Ecosystem of payment devices, applications, infrastructure and users

Confidential Property of CampusGuard

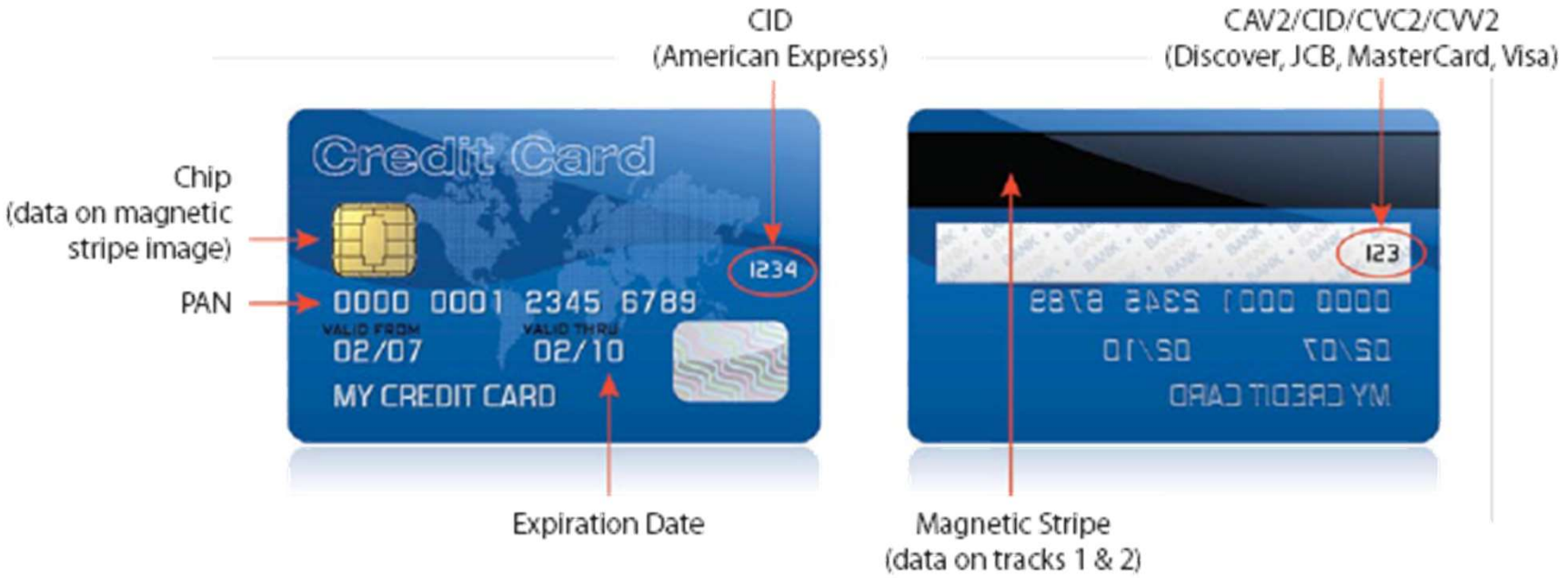
PCI DSS: 6 Goals, 12 Requirements



Control Objective	Requirements
1. Build and maintain a secure network	1. Install and maintain a firewall configuration to protect data 2. Change vendor-supplied defaults for system passwords and other security parameters
2. Protect cardholder data	3. Protect stored data 4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks
3. Maintain a vulnerability management program	5. Use and regularly update antivirus software 6. Develop and maintain secure systems and applications
4. Implement strong access control measures	7. Restrict access to data to a need-to-know basis 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
5. Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
6. Maintain an information security policy	12. Maintain a policy that addresses information security

Confidential Property of CampusGuard

What is the PCI DSS trying to protect?



Confidential Property of CampusGuard

Covered Data Elements



1st 6 / Last 4 OK

Only considered CHD if full PAN stored

	Data Element	Storage Permitted	Protection Required
der	PAN	Yes	Yes
	Cardholder name	Yes	No
	Service code	Yes	No
	Expiration date	Yes	No
Sensitive authentication data	Magnetic stripe	No	No storage permitted
	CVC2/CVV2/CID	No	No storage permitted
	PIN/PIN block	No	No storage permitted

Confidential Property of CampusGuard

Merchant Levels

Level	VISA / MasterCard / DISCOVER	American Express
1	> 6 million Visa/MC txns/yr	> 2.5 million transactions/yr
2	1 to 6 million Visa/MC txns/yr	50,000 to 2.5 million txns/yr
3	20,000 to 1 million Visa/MC ecommerce txns/yr	All other Amex merchants
4	All other Visa/MC merchants	N/A

Confidential Property of CampusGuard

Merchant Levels and Validation

Level	VISA / MasterCard / DISCOVER	
1	• Annual on-site assessment (QSA) • Quarterly network scan (ASV)	• Annual on-site assessment (QSA) • Quarterly network scan (ASV)
2	• Annual on-site assessment (QSA/ISA) • Quarterly network scan (ASV)	• Quarterly network scan (ASV)
3	• Annual Self-Assessment Questionnaire (SAQ) • Quarterly network scan (ASV)	• Quarterly network scan (ASV)
4	• At discretion of acquirer/card brand • Annual SAQ • Quarterly network scan (ASV)	▪ N/A

Confidential Property of CampusGuard

Payment Methods & Validation Requirements

SAQ Type	Questions	Payment Method
A	**22**	Card-not-present merchants; all cardholder data functions fully outsourced to validated third parties
A-EP	**191**	Partially outsourced ecommerce merchants using validated third party websites for payment processing
B	**41**	Merchants with only imprint machines or only standalone, dial-out terminals – No electronic cardholder data storage
B-IP	**82**	Merchants with standalone, IP-connected PTS-approved Point-of-Interaction (POI) terminals – No electronic CHD storage
C	**160**	Merchants with payment application systems connected to the Internet – No electronic CHD storage
C-VT	**79**	Merchants with web-based virtual terminals hosted by validated third parties – No electronic CHD storage
D	**329**	All other SAQ-eligible merchants
D-SP	**354**	All SAQ-eligible service providers
P2PE	**33**	PCI Council listed P2PE solutions only, with POI terminals approved for the solution – No electronic CHD storage

Confidential Property of CampusGuard

Common PCI DSS Myths

- "I can wait until the bank asks me to be compliant." –or– "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)



Confidential Property of CampusGuard

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

Confidential Property of CampusGuard

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.



Confidential Property of CampusGuard

Who Must Comply?

Do you….

- Store, process or transmit cardholder data?
  - Point-of-Sale (POS)
  - Mail Order/Telephone Order (MOTO)
  - FAX
  - Ecommerce (website where customer can input their credit card information to complete a transaction)
- Use a system that processes or stores credit card data?
  - And are other systems connected to them?

IF YOU ANSWER YES TO ANY OF THE ABOVE QUESTIONS THEN PCI DSS APPLIES TO YOU!

Confidential Property of CampusGuard

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*

Confidential Property of CampusGuard

New in PCI DSS 3.x

- Clarification re: scope
- Business-as-Usual
- Policies and procedures
- New SAQs
- Data flow diagram now required (1.1.3)
- Removal of SSL and early TLS (2.2.3, 2.3, 4.1)
- 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)

Confidential Property of CampusGuard

New in PCI DSS 3.x

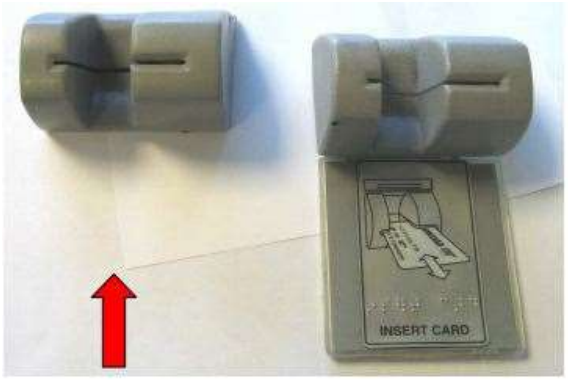


- Use multi-factor authentication for non-console administrative access to the CDE (8.3.1)
- Increased rigor for penetration testing, including validation of any segmentation (11.3)
- Response process for change-detection (a.k.a. file-integrity monitoring) alerts (11.5)
- Formal, documented analysis of risk (12.2)
- Maintain information about which PCI DSS requirements are managed by each service provider (12.8.5)
- Service providers must provide written acknowledgement (12.9)

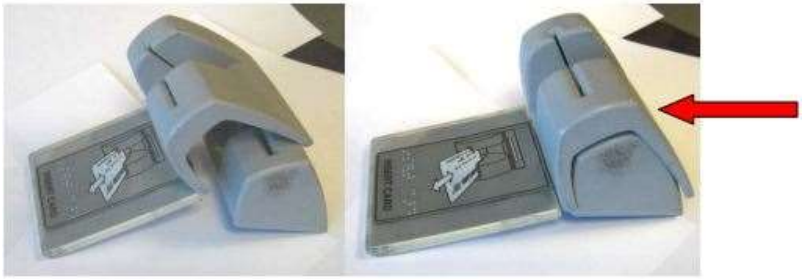
Confidential Property of CampusGuard

Why Requirement 9.9?

- Device skimming is sadly not rare



The real card reader slot. The capture device



The side cut out is not visible when on the ATM.

Images from www.krebsonsecurity.com

18 Point-of-Sale Skimmers: Robbed at the Register

MAY 11

Michaels Stores said this month that it had replaced more than 7,200 credit card terminals from store registers nationwide, after discovering that thieves had somehow modified or replaced machines to include point of sale (POS) technology capable of siphoning customer payment card data and PINs. The specific device used by the criminal intruders has not been made public. But many devices and services are sold on the criminal underground to facilitate the surprisingly common fraud.

POS skimmers typically are marketed and sold in one of three ways: Pre-compromised POS terminals that can be installed at the cash register; Fake POS devices that do not process transactions but are designed to record data from swiped cards and PIN entries; or Do-it-yourself kits that include all parts, wiring and instructions needed to modify an existing POS terminal.



POS skimmer component. Bogus PIN pad connector is at left.

I spoke at length to a POS skimmer seller who has been peddling POS modification

Confidential Property of CampusGuard

Requirement 9.9







Confidential Property of CampusGuard

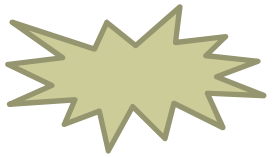
Securing Points of Interaction

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



Information Supplement

Skimming Prevention:
Best Practices for Merchants
Version 2.0



Confidential Property of CampusGuard

EMV: How Does it Fit?

- EMV is a separate standard
  - Chip & PIN vs. Chip & Signature
  - Supports PCI DSS in a layered security approach
  - Protects against card fraud
  - Affects only physical points of interaction
  - Does not encrypt the primary account number
  - Pushes fraud to other payment channels

Confidential Property of CampusGuard

Defining Your PCI DSS Scope



- People, processes, and technologies that store, process, **or** transmit cardholder data, or that *could affect* the security of those components that do touch the data. Simple, right?
  - Servers (web, database, virtual, etc.), and workstations
  - Firewalls, IDS/IPS
  - Network switches, routers, load balancers, etc.
  - Network attached storage or connected arrays
  - Name resolution, time sync, authorization.

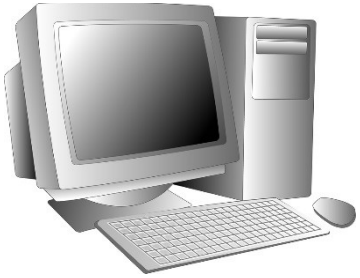
Confidential Property of CampusGuard

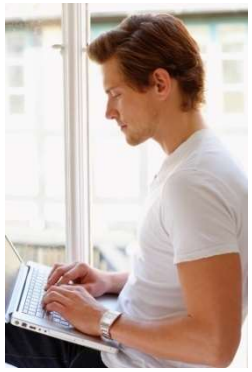
What's in PCI Scope?



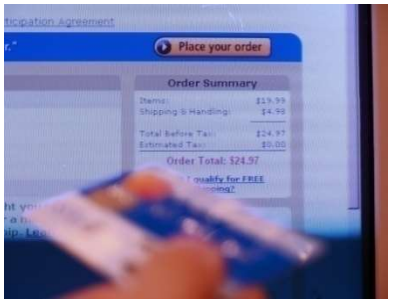
Card Swipe Machine?

Office Workstations?





Student?



Shopping Cart?



Computer Lab?

Phone Transaction?



Confidential Property of CampusGuard

3rd Party Payment Systems

- Many colleges and universities adopt the use of a 3rd party processor or payment system for tuition and other payments.
  - **Great idea**
  - **Limits scope for the PCI DSS**
  - **Designed to be hands-off at the school**
- Purchasing of PA-DSS compliant systems
  - **Can help in compliance effort**
  - **Not a panacea**

Confidential Property of CampusGuard

What can go wrong?

- What happens when an employee enters data for the customer on their machine?
  - The DSS is very definitive about transmission of CHD
    - Employees' workstation and the network its connected to comes into scope
      - Unnecessary software
      - Monitoring
      - Associated systems
      - If not segmented from the rest of the network, the rest of the school comes into scope.

Confidential Property of CampusGuard

Outside Payment Processing

- Using a 3rd party to process payments for the institution may alleviate some scope and PCI DSS requirement considerations.
  - Conference registrations, day camps, T-shirt sales etc.
  - Sites that contain a “Pay Now” button that redirects or uses embedded code to a 3rd party.
- You can never outsource your ultimate PCI compliance responsibility
- Unless the entire site is fully hosted by a PCI compliant provider, compliance obligations for the webserver that hosts the site with the “Pay Now” button can fall under SAQ A-EP.

Confidential Property of CampusGuard

What About Mobile Payments?

MasterCard and Visa both have statements for Merchants wishing to use Mobile Point Of Sale (MPOS) devices



“Due to the inherent security limitations of mobile devices, the PCI SSC is **not** certifying MPOS payment applications that reside on multi-purpose, consumer mobile devices (referred to by the PCI SSC as a Mobile Payment Acceptance Application Category 3) until further guidance is developed to ensure the security of cardholder data within the mobile device. Please refer to the PCI SSC Website for more information.”

(*MasterCard statement on Mobile payments)*

Confidential Property of CampusGuard

Mobile Payment Alternatives

- Purpose built cellular POS device
  - VeriFone VX520
  - Ingenico iWL250
  - Etc.





Confidential Property of CampusGuard

2017 Data Breach Investigations Report

10th Edition



Confidential Property of CampusGuard

DBIR: Incident Classification

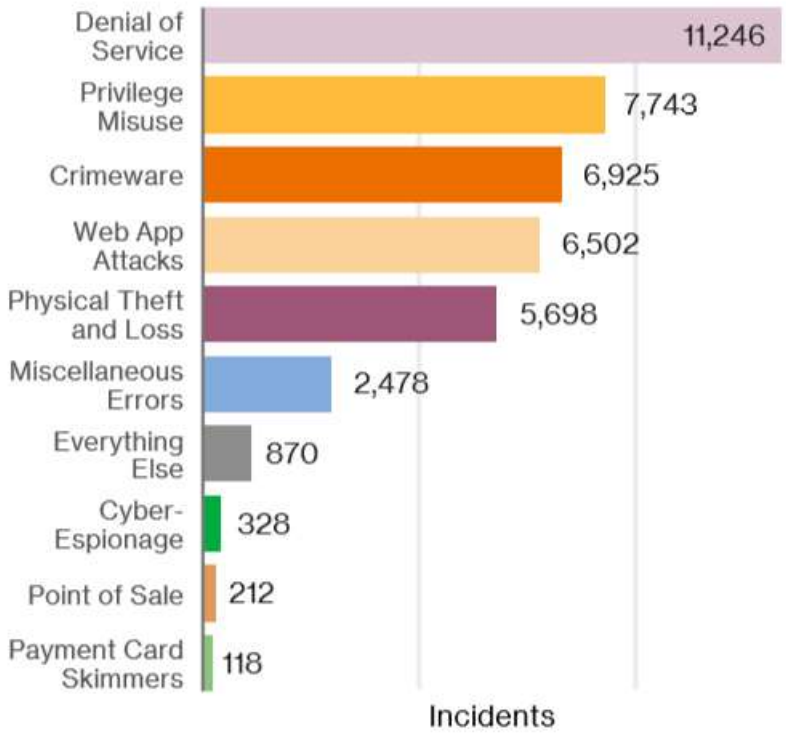


Figure 34: Percentage and count of incidents per pattern (n=42,068)

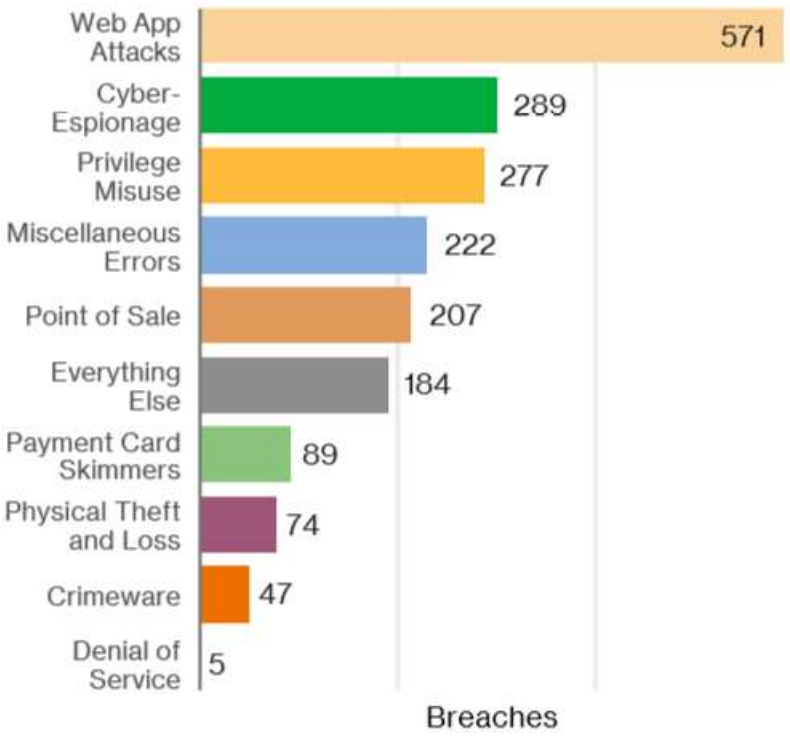


Figure 33: Percentage and count of breaches per pattern (n=1,935)

Confidential Property of CampusGuard

DBIR: Educational Services

Frequency	455 incidents, 73 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Miscellaneous Errors and Everything Else represent 67% of all data breaches within Education
Threat actors	71% External, 30% Internal, 3% Partner (breaches)
Actor motives	45% Financial, 43% Espionage, 9% Fun (breaches)
Data compromised	56% Personal, 27% Secrets, 8% Credentials
Summary	This section will focus on confirmed data breaches, but Education remains a consistent target of Denial of Service (DoS) attacks also. 2016 results reflect a substantial increase in the number of espionage-related breaches.

The data showed that state-affiliated actors (involved in over half of the breaches) were targeting these educational institutions. We also saw a handful of breaches where organized criminal groups were involved with their mind on the money (and the money on their mind).

The threat categories that were the real troublemakers within the patterns mentioned above were hacking, social and malware.

Confidential Property of CampusGuard

DBIR: Educational Services

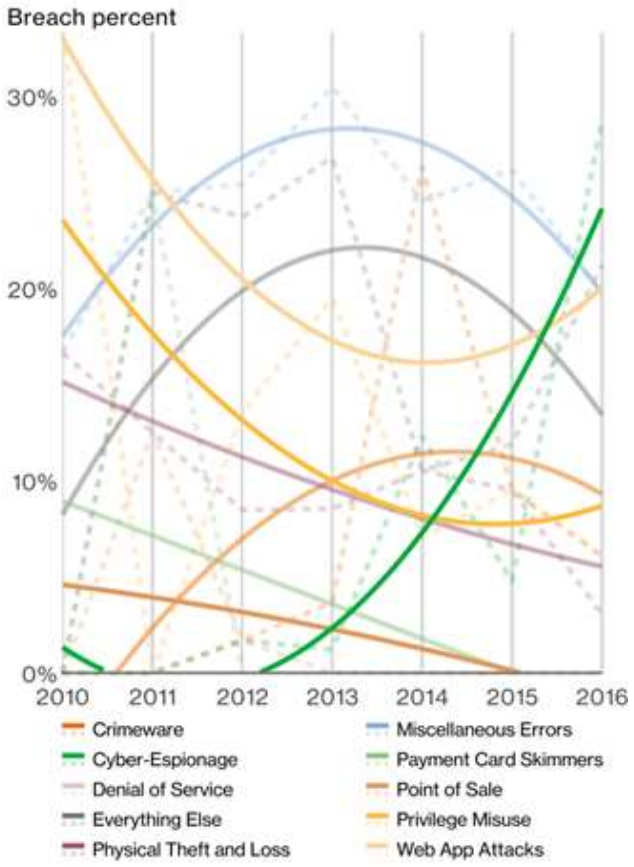


Figure 17: Frequency of incident classification patterns over time within Education breaches

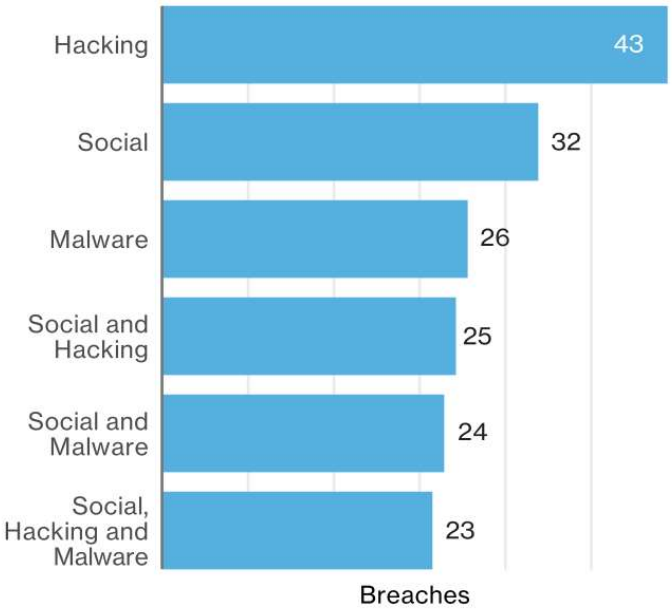
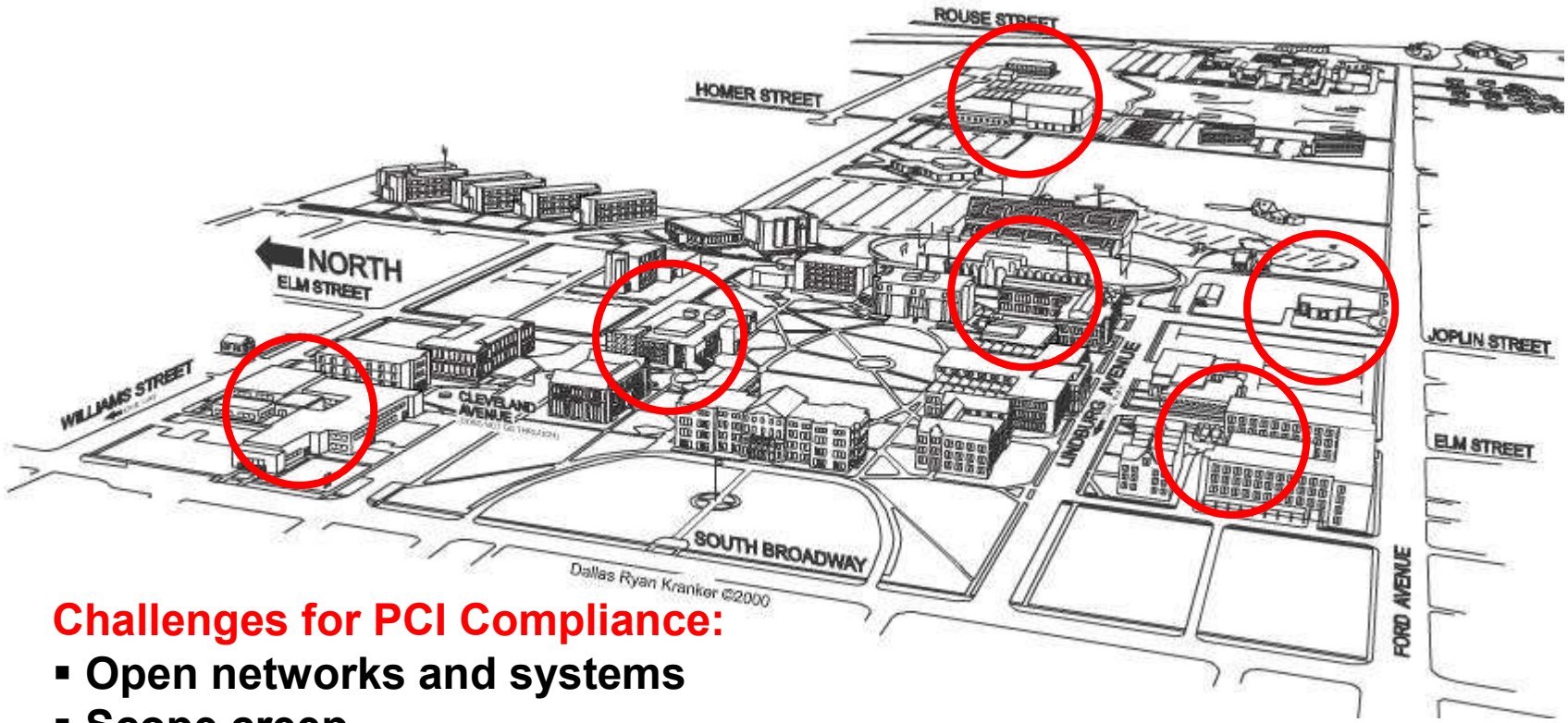


Figure 18: Relationships between actions within Education breaches (n=73)

Confidential Property of CampusGuard

A Campus Is A “City"



Challenges for PCI Compliance:

- **Open networks and systems**
- **Scope creep**
- **Overloaded staff**
- **Fiscal constraints**

Confidential Property of CampusGuard

PCI Non-Compliance

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)

Confidential Property of CampusGuard

News Travels Fast: Do you want to be in it?



SECURITY

UC Berkeley Servers Hacked, 1,600 May be Affected in Breach

The data breach included about 1,300 Social Security numbers and 300 credit card numbers, according to a campus spokeswoman.

BY NATALIE NEYSA ALUND, THE DAILY REVIEW / DECEMBER 17, 2014

(TNS) -- UC Berkeley officials are notifying about 1,600 people that their personal information may have been hacked by someone who gained access to servers and databases in the campus's Real Estate Division earlier this year.

The data breach included about 1,300 Social Security numbers and 300 credit card numbers, said campus spokeswoman Janet Gilmore.

Many of those affected are current or former campus employees. The group also includes people with companies doing business with the division from the early 1990s through May 2014, Gilmore said.

CAMPUS & COMMUNITY, CAMPUS NEWS, W

Campus alerting 80,000 individuals to cyberattack

By Janet Gilmore, Public affairs | FEBRUARY 26, 2016

UC Berkeley officials are sending alert notices to approximately 80,000 current and former faculty, staff, students and vendors following a criminal cyberattack on a system storing their Social Security or bank account numbers.

Confidential Property of CampusGuard

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
- Become a level 1 merchant

10,000 accounts X ~$225 / account = $2.25 Million

Reputation – Priceless!

Confidential Property of CampusGuard

Some Best Practices



- NEVER email credit card information
- NEVER store credit card numbers in any database or spreadsheet
- Mask all but last 4 digits of cc number
- Keep credit card documentation locked in a safe or SECURE filing cabinet
- Permit only those employees who have a legitimate “need-to-know” access to cardholder info
- Don’t allow unauthorized persons access to areas where credit card data is stored

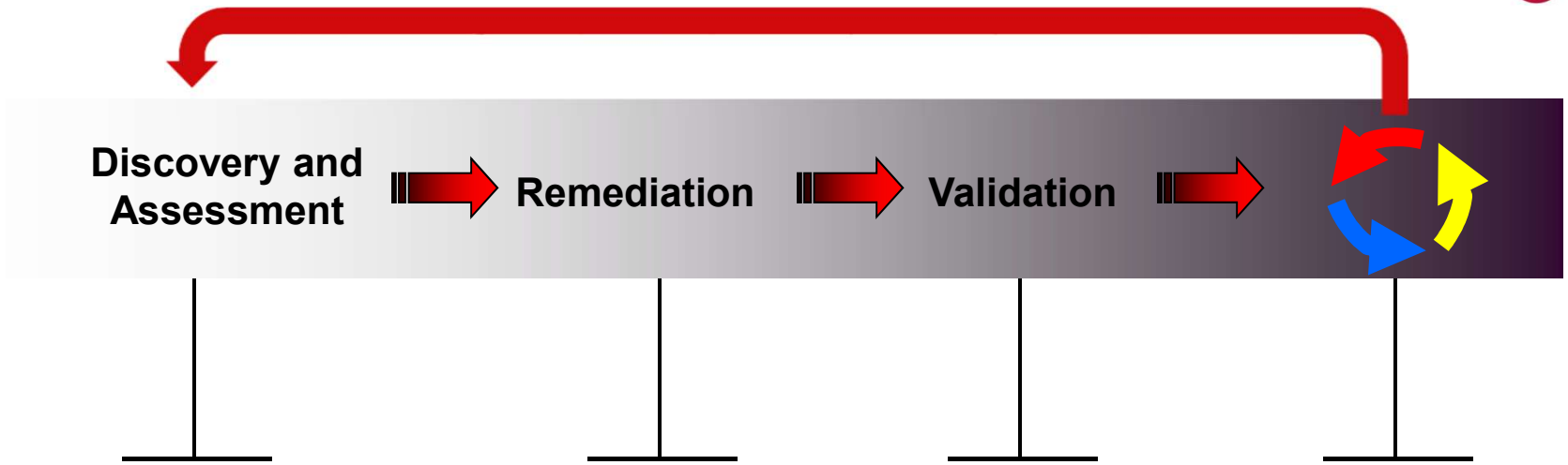
Confidential Property of CampusGuard

Some Best Practices

- Destroy documentation containing credit card information when no longer needed for business or legal reasons
- Document departmental desktop procedures
  - Update cash handling procedures
- Segregate duties – the individual performing reconciliation should not be involved in processing credit card sales or refunds

Confidential Property of CampusGuard

PCI DSS is a Process



- 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

Confidential Property of CampusGuard

Resources

- PCI Security Standards Council
  - www.pcisecuritystandards.org/
- Card Brands
  - www.visa.com/cisp
  - www.mastercard.com/sdp
- Privacy Rights Clearinghouse
  - http://www.privacyrights.org/
- Ponemon Institute
  - http://www.ponemon.org/
- CampusGuard
  - www.campusguard.com/

Confidential Property of CampusGuard

Northwestern



Pete Campbell, CISA, QSA
Security Advisor
CampusGuard
+1.479.435.6886
pcampbell@campusguard.com

Confidential Property of CampusGuard