



PCI DSS Merchant Training

Jarvis Gilmore, CISSP, QSA
Security Advisor
CampusGuard



CampusGuard Services

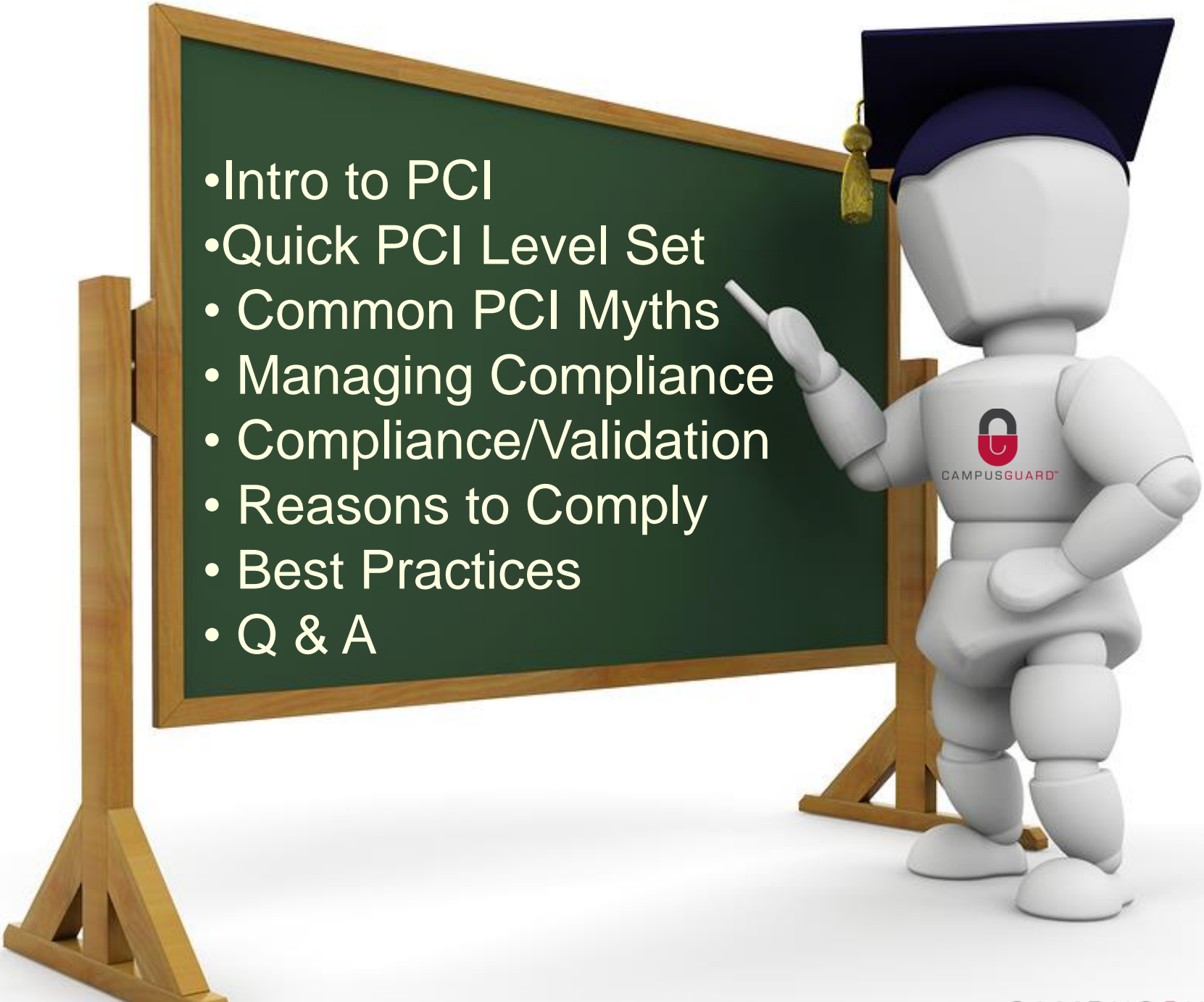
- Assessments
- Annual Support
- Offensive Security Services
- Training
- Audits

Information Security

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

Compliance

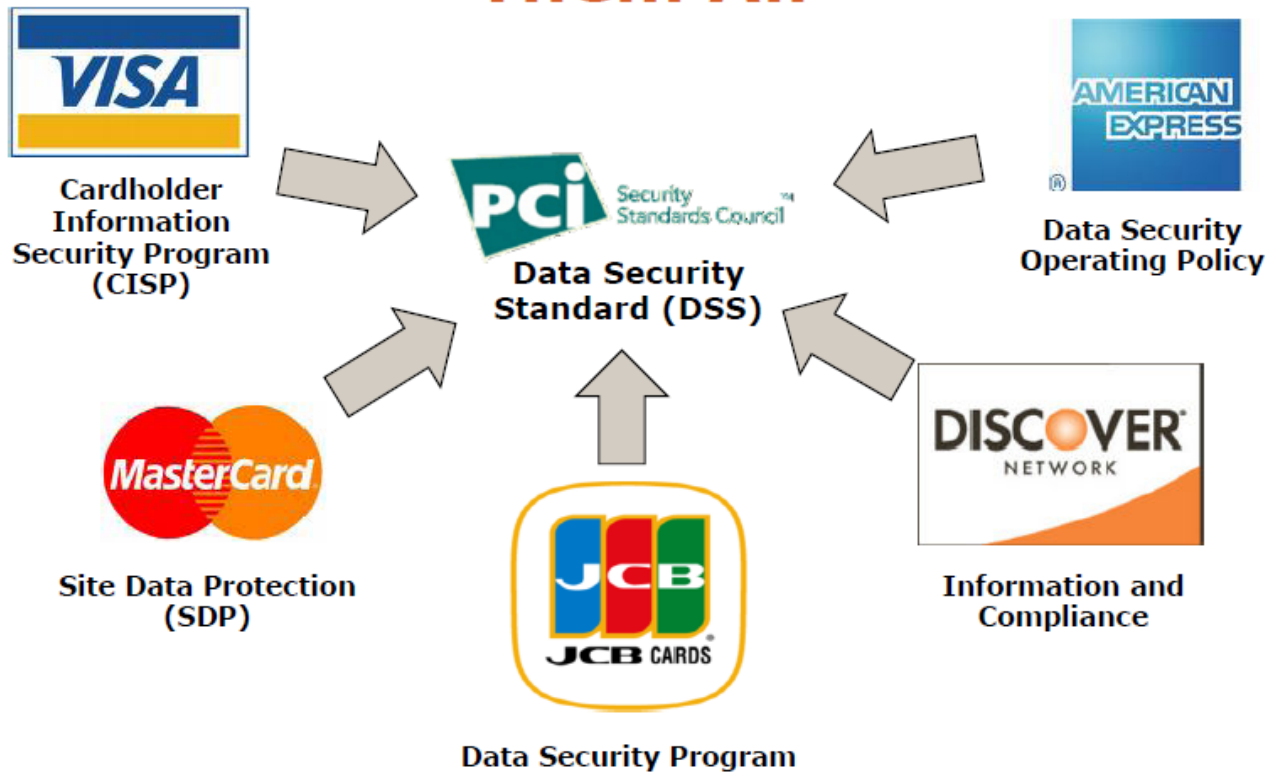
- PCI DSS
- GLBA
- NACHA/ACH
- HIPAA and HITECH
- GDPR
- FERPA
- FACTA

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

Payment Card Industry Data Security Standard (PCI DSS)



PCI DSS: "One Standard to Rule Them All"



The PCI SSC



- Maintains all PCI compliance validation documentation
 - Payment Card Industry Data Security Standard (PCI DSS)
 - Merchants
 - SAQs (level 3 & 4)
 - Report on Compliance (Level 1 & 2)
 - Service Providers
 - SAQ D for Service providers (level 2)
 - Report on Compliance for Service providers (level 1)
- Certifications
 - Forensic Investigators (FI)
 - Qualified Security Assessors (QSA, PA-QSA, P2PE-QSA)
 - Internal Security Assessor (ISA)
 - Approved Scanning Vendors (ASV)
 - Payment Card Industry Professional (PCIP)
 - Qualified Integrators and Resellers (QIR)
 - Others

The PCI SSC



- Validations
 - PIN Transaction Security (PTS)
 - Point-to-Point Encryption (P2PE)
 - Payment Application Data Security Standard (PA-DSS)
 - Acquirers
- Training
 - PCI Awareness
 - Webinars
- Guidance
 - Supporting Documents
 - Glossary of Terms
 - Prioritized Approach
 - Quick Reference Guides

Who Must Comply?

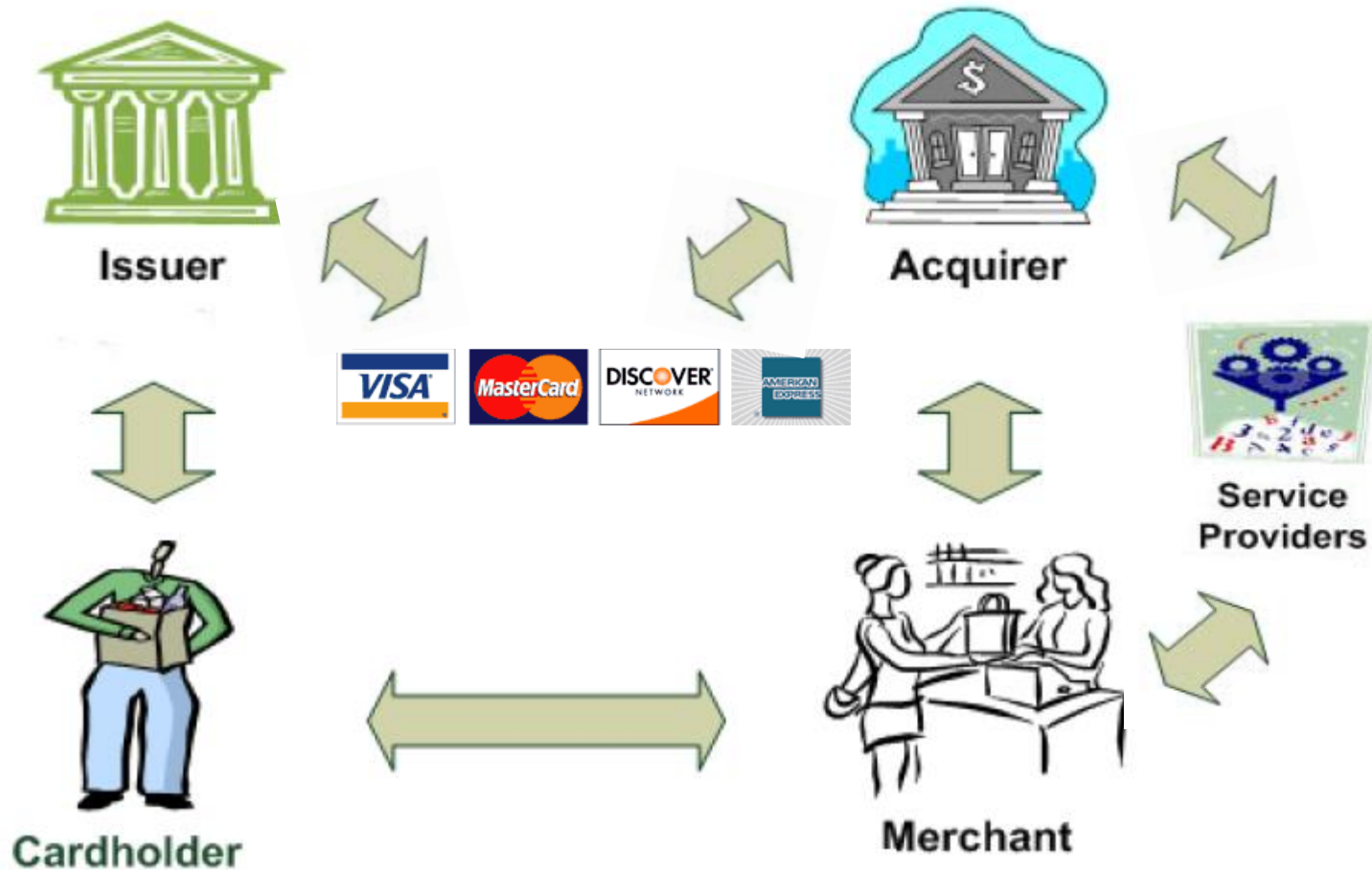


Do you....

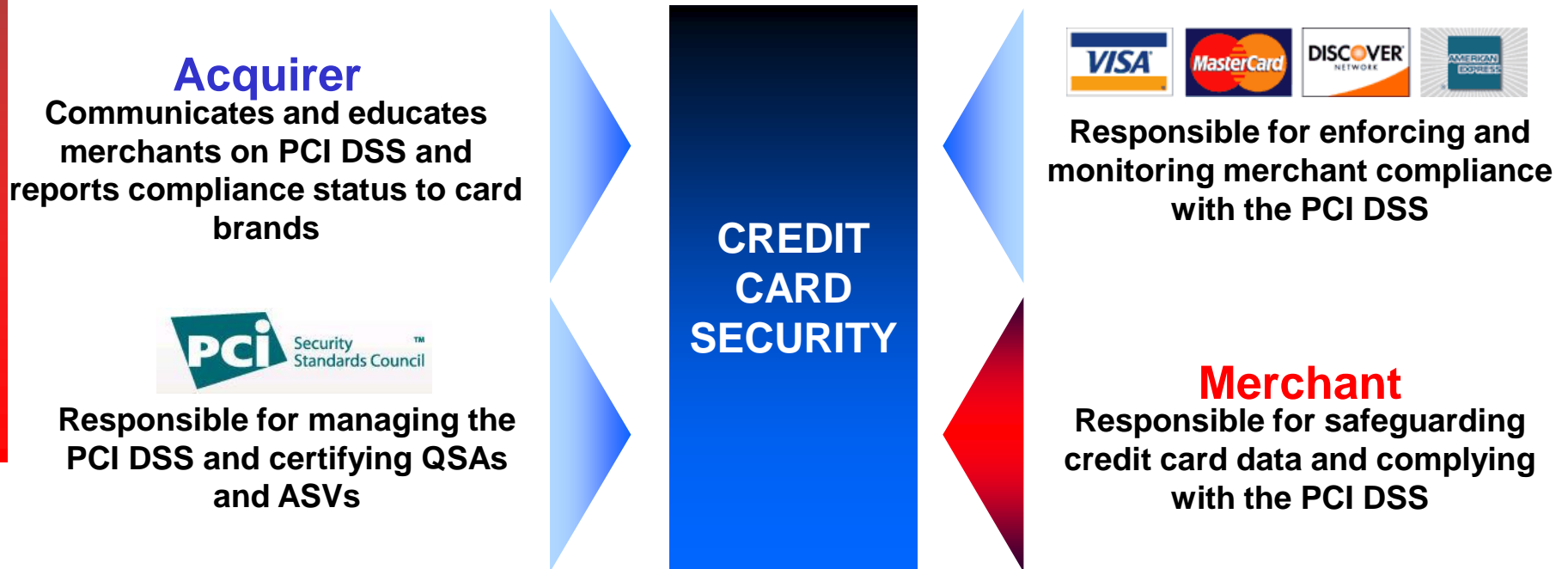
- Store, process or transmit cardholder data?
 - Point-of-Sale (POS)
 - Mail Order/Telephone Order (MOTO)
 - FAX
 - Ecommerce (website where customer can input their credit card information to complete a transaction)
- Use a system that processes or stores credit card data?
 - And are other systems connected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

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

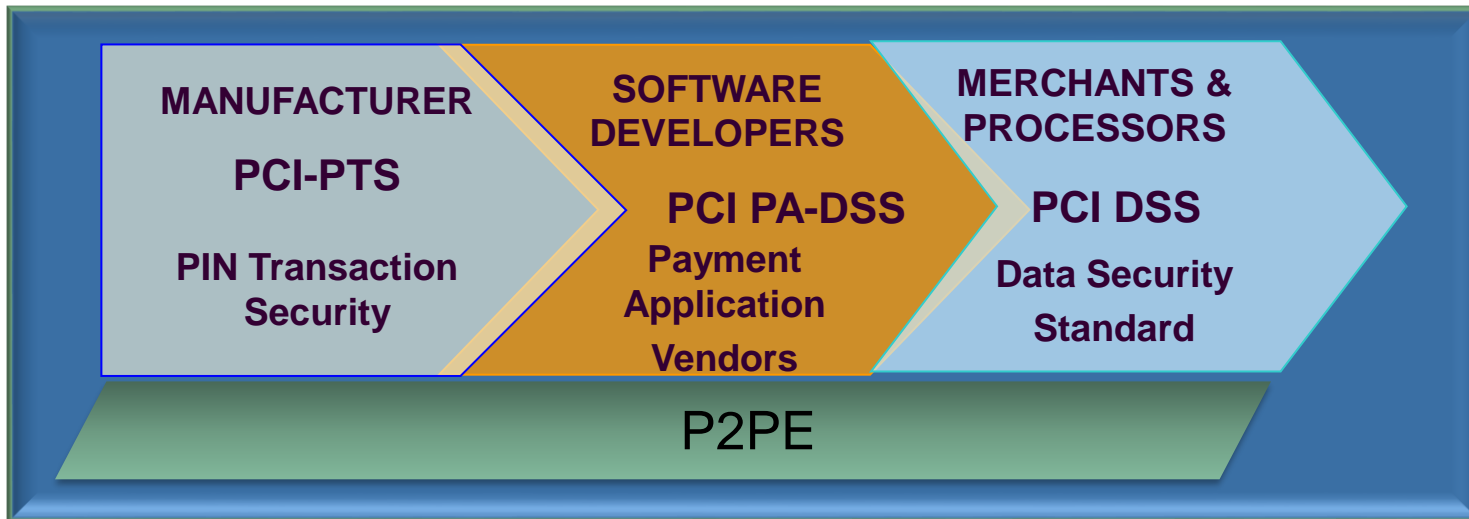
Players in the Payment Lifecycle



PCI Relationships



PCI = Multiple Standards



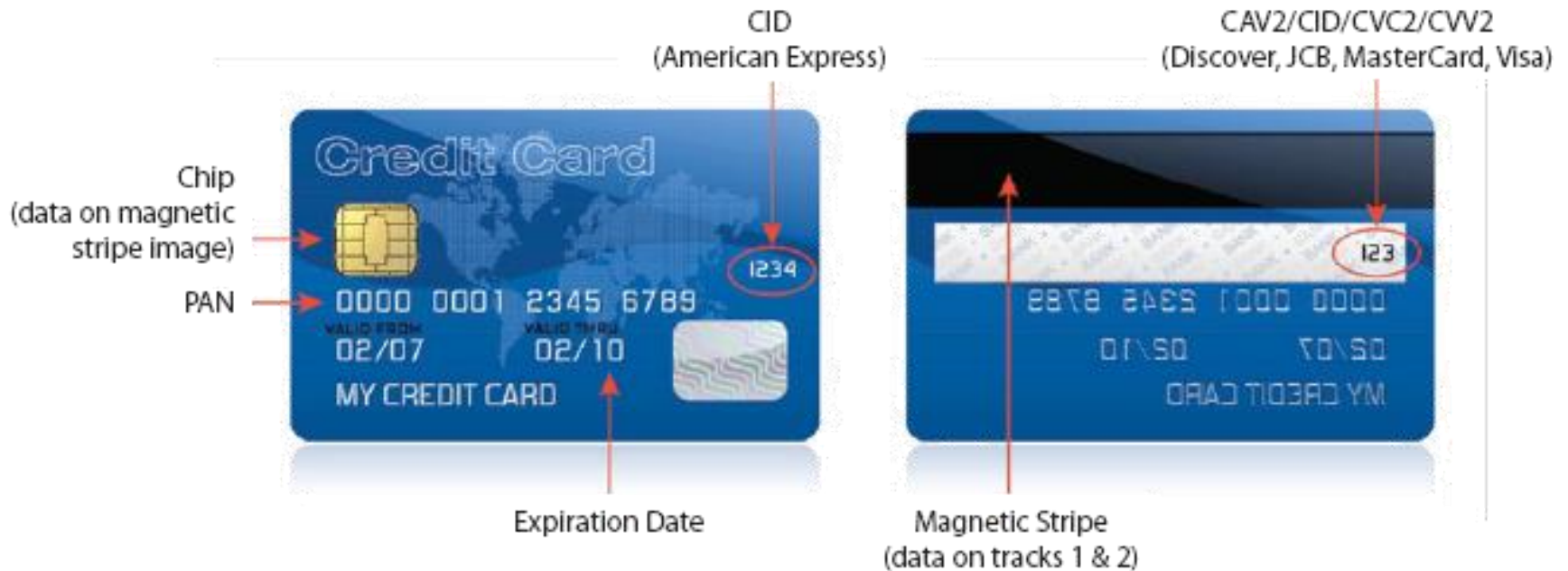
Ecosystem of payment devices, applications, infrastructure and users

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

What is the PCI DSS trying to protect?







Covered Data Elements



1 st 6 / Last 4 OK	Data Element	Storage Permitted	Protection Required
Cardholder data Only considered CHD if full PAN stored	PAN	Yes	Yes
	Cardholder name	Yes	No
	Service code	Yes	No
	Expiration date	Yes	No
Sensitive authentication data	Magnetic stripe/Track equivalent (chip)	No	No storage permitted
	CVC2/CVV2/CID	No	No storage permitted
	PIN/PIN block	No	No storage permitted





Merchant Levels



Level	  	
1	<p>> 6 million Visa/MC txns/yr</p>	<p>> 2.5 million transactions/yr or if you've been designated a Level 1 by American Express</p>
2	<p>1 to 6 million Visa/MC txns/yr</p>	<p>50,000 to 2.5 million txns/yr</p>
3	<p>20,000 to 1 million Visa/MC ecommerce txns/yr</p>	<p>10,000 to 50,000 million txns/yr</p>
4	<p>All other Visa/MC merchants</p>	<p>All other Amex merchants</p>

Merchant Levels and Validation



Level	  	
1	<ul style="list-style-type: none"> • Annual on-site assessment (QSA, RoC) • Quarterly network scan (ASV) 	<ul style="list-style-type: none"> • Annual on-site assessment (QSA, RoC) • Quarterly network scan (ASV)
2	<ul style="list-style-type: none"> • Annual on-site assessment (QSA/ISA) • Quarterly network scan (ASV) 	<ul style="list-style-type: none"> • Quarterly network scan (ASV)
3	<ul style="list-style-type: none"> • Annual Self-Assessment Questionnaire (SAQ) • Quarterly network scan (ASV) 	<ul style="list-style-type: none"> • Quarterly network scan (ASV)
4	<ul style="list-style-type: none"> • At discretion of acquirer/card brand, except for Visa • Annual SAQ • Quarterly network scan (ASV) 	<ul style="list-style-type: none"> ▪ N/A

Payment Methods & Validation Requirements

SAQ Type	Questions	Payment Method
A	24	Card-not-present merchants; all cardholder data functions fully outsourced to validated third parties
A-EP	192	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	87	Merchants with standalone, IP-connected PTS-approved Point-of-Interaction (POI) terminals – No electronic CHD storage
C	162	Merchants with payment application systems connected to the Internet – No electronic CHD storage
C-VT	84	Merchants with web-based virtual terminals hosted by validated third parties – No electronic CHD storage
P2PE	33	PCI Council listed P2PE solutions only, with POI terminals approved for the solution – No electronic CHD storage
D	330	All other SAQ-eligible merchants
D-SP	364	All SAQ-eligible service providers

Common PCI DSS Myths



- Outsourcing credit card acceptance does not mean that you have no PCI compliance requirements.

You may have outsourced your technical controls to a service provider, but there are still administrative controls in PCI scope.

Check out all of requirement 12.

Common PCI DSS Myths



- No matter how often or how much credit card data you handle.
- Whether you touch or do not touch credit cards in the process.



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

Common PCI DSS Myths



- PCI requirements must be fully to be compliant.
- Answer “Yes” or “Not Applicable”.
- Any “No” answers means Not Compliant



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*

Check Devices



- Skimming is sadly not rare



Image from www.krebsonsecurity.com



Image from www.engadget.com

Check Devices



Check Devices



- Skimming is sadly not rare



Image from www.collbuster.net



Image from www.desmoinesregister.com

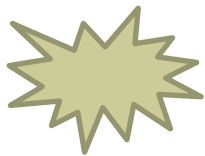
Teamwork: Skimmer Installation



Securing Points of Interaction



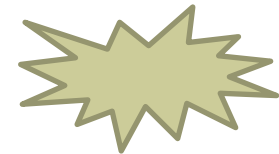
- Maintain an inventory list of devices
- Periodically inspect devices to look for tampering or substitution
- Train personnel to be aware of suspicious behavior and to report tampering/substitution



Information Supplement

Skimming Prevention: Best Practices for Merchants

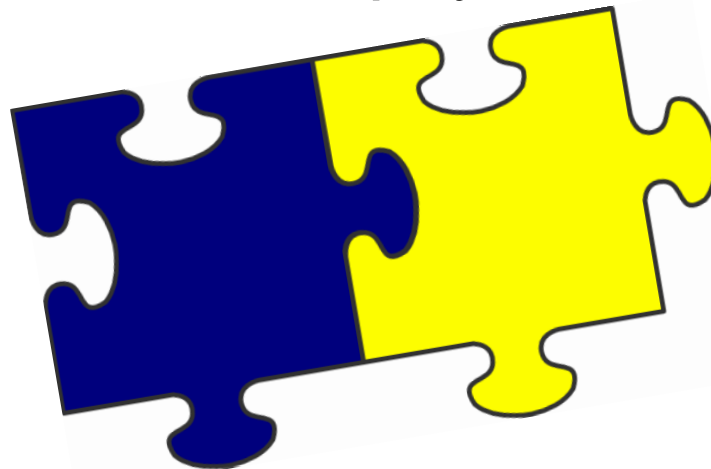
Version 2.0



EMV: How Does it Fit?



- 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



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.
- “At a high level, scoping involves the identification of people, processes, and technologies that interact with or could otherwise impact the security of CHD.”¹
- Any systems that reside in or connect to the CDE.

¹ Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation

What's in PCI Scope?



**Credit Card Reader
Pin Pad**



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.
 - 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**
- Only some integration methods qualify for easy SAQs. Many common ecommerce implementations will need to be assessed under much longer and complicated SAQs.

What can go wrong?



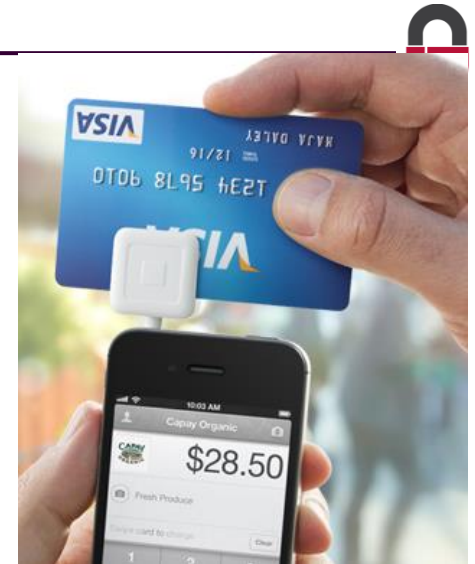
- What happens when employees enter data for the customer on their machines?
 - Risk of data loss (breach) increases
 - PCI scope is immediately increased
 - Compliance requirements increase
 - Cost of compliance increases
 - Requires more IT involvement
 - May go against written overarching policies

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)



Mobile Payment Alternatives



- ❖ Purpose built cellular POS device
 - xAPT-103P
 - Move/5000 (Ingenico)
 - T650p (VeriFone)



Mobile Payment Alternatives



❖ P2PE Solutions on mobile devices

ID Tech
SRED Key 2



Verifone
Carbon Mobile 5



First Data
Clover Flex



PAX
a920



Version Data Breach Investigations Report

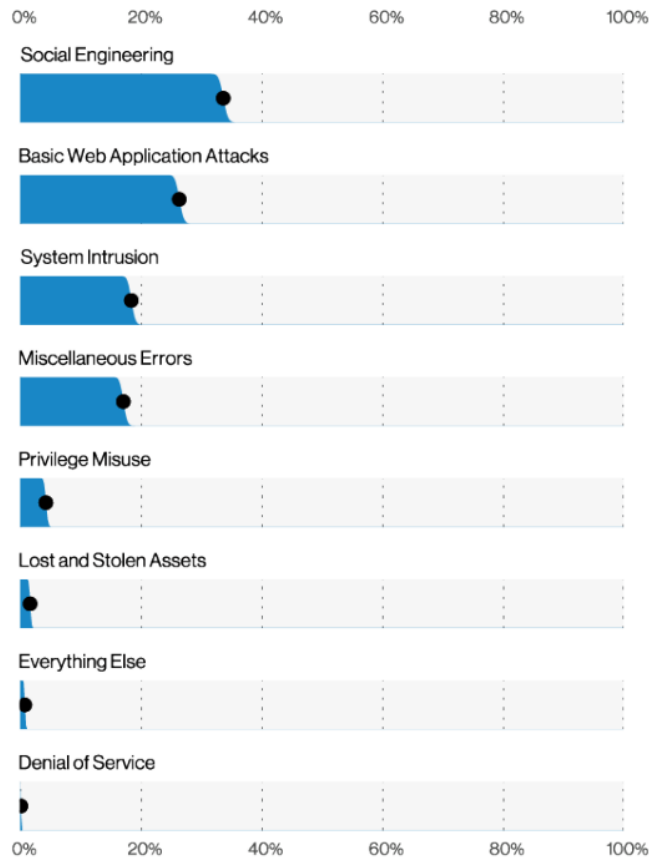


Figure 5. Patterns in breaches (n=5,275)

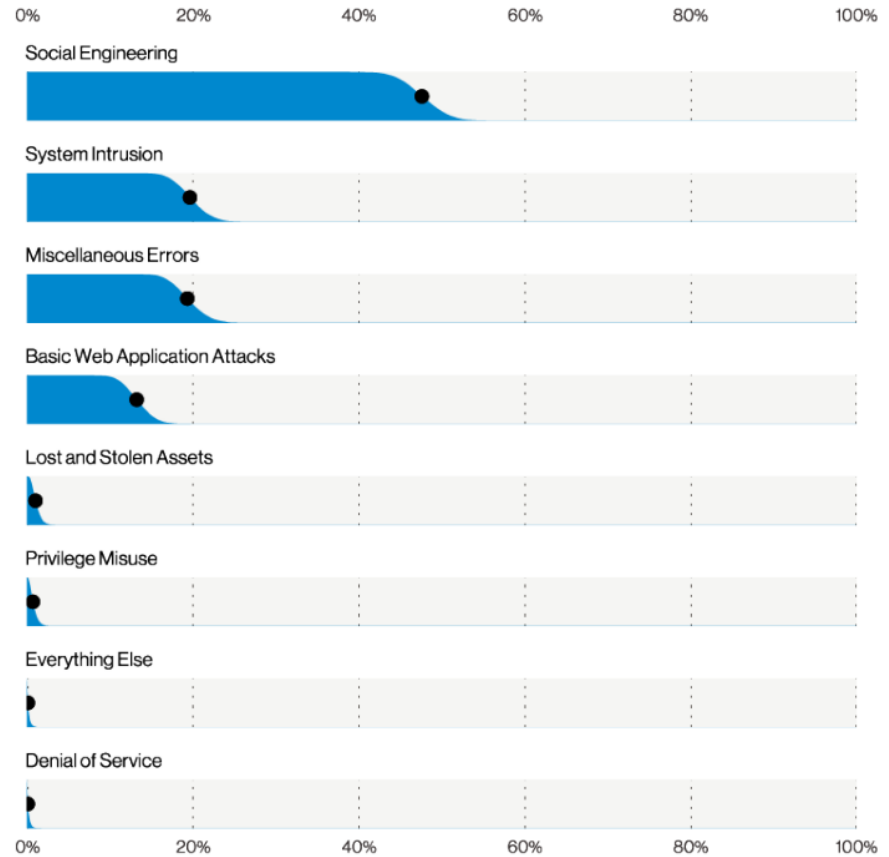


Figure 101. Patterns in Education breaches (n=344)

Weakest Link: People

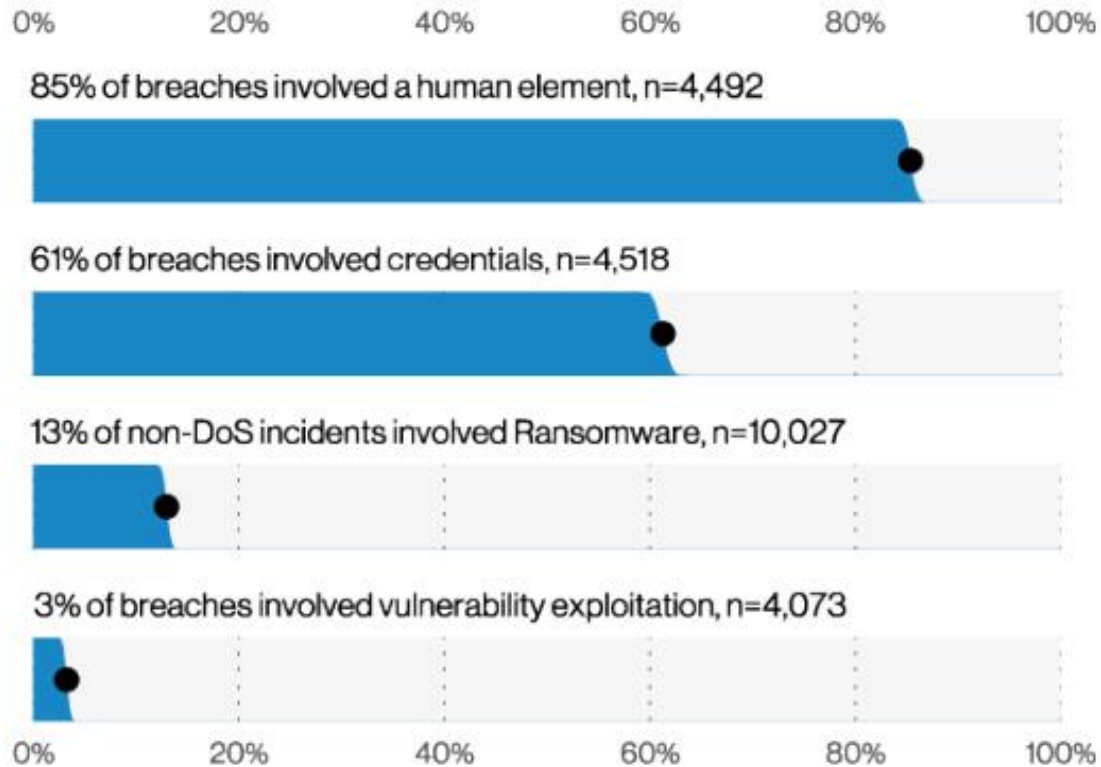
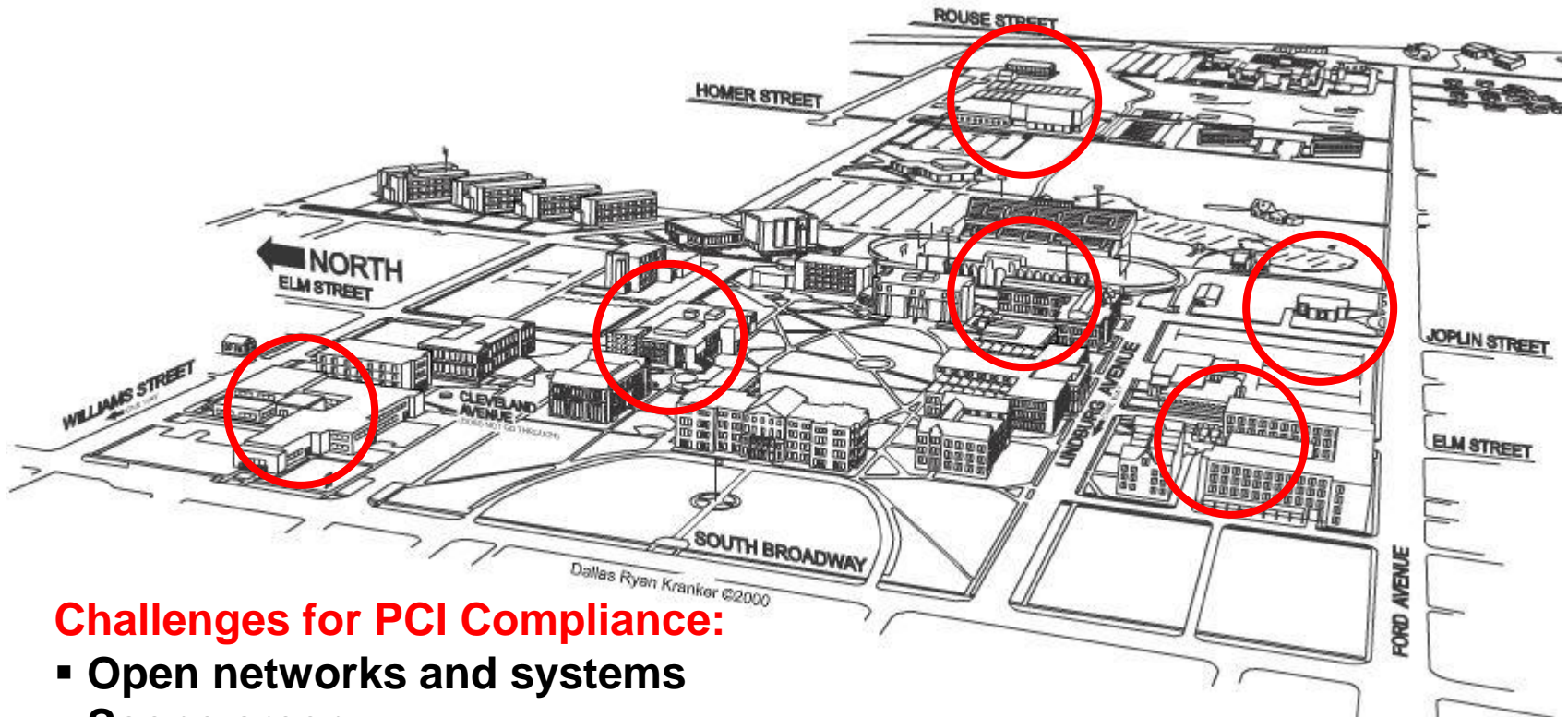


Figure 7. Select action varieties (n=4,073)

A Campus Is A "City"



Challenges for PCI Compliance:

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

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)**

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

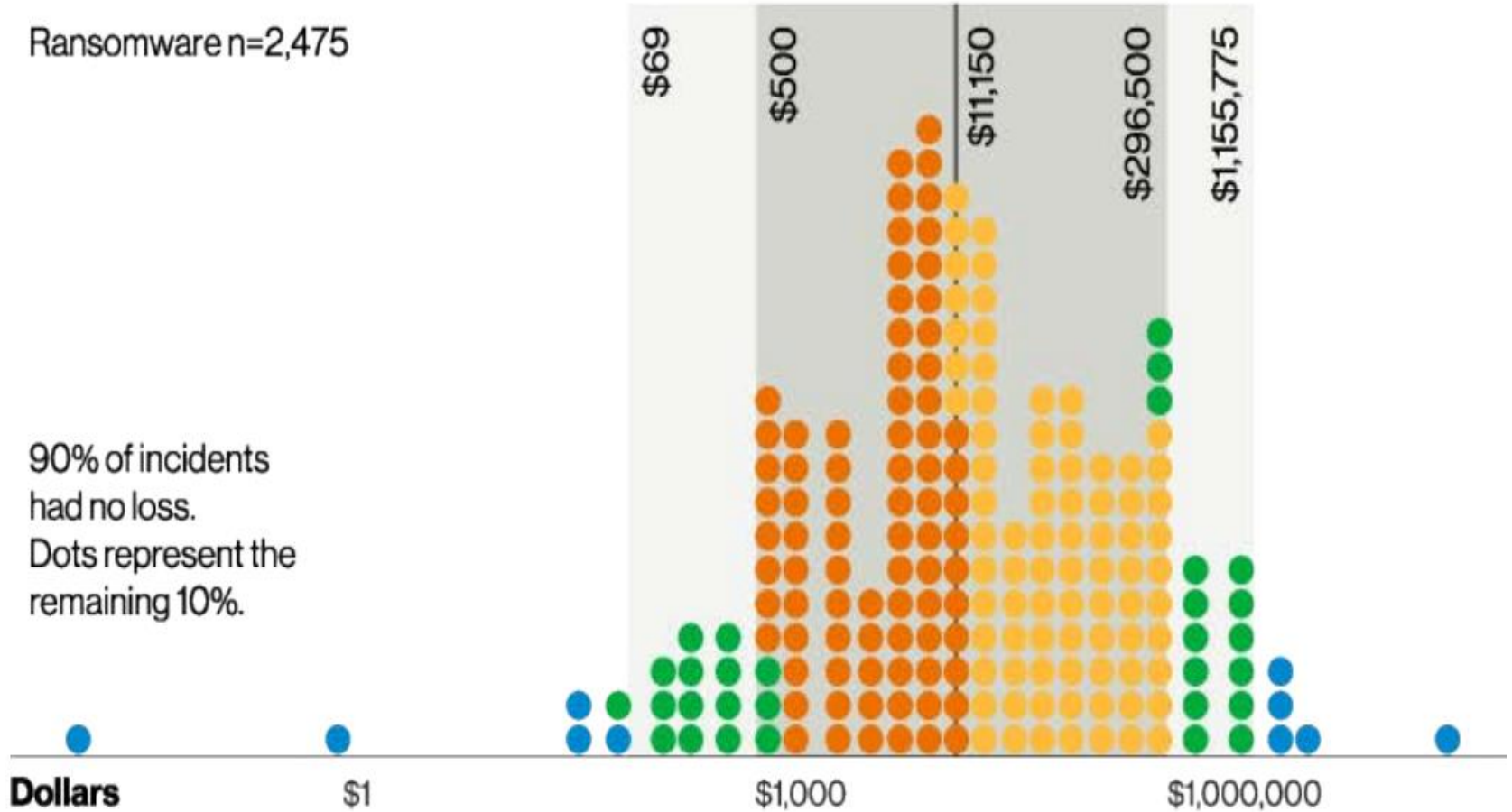
Reputation – Priceless!

Impact Examples



Ransomware n=2,475

90% of incidents had no loss.
Dots represent the remaining 10%.



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



Books

Grad



"We want to assure you that we understand exactly what

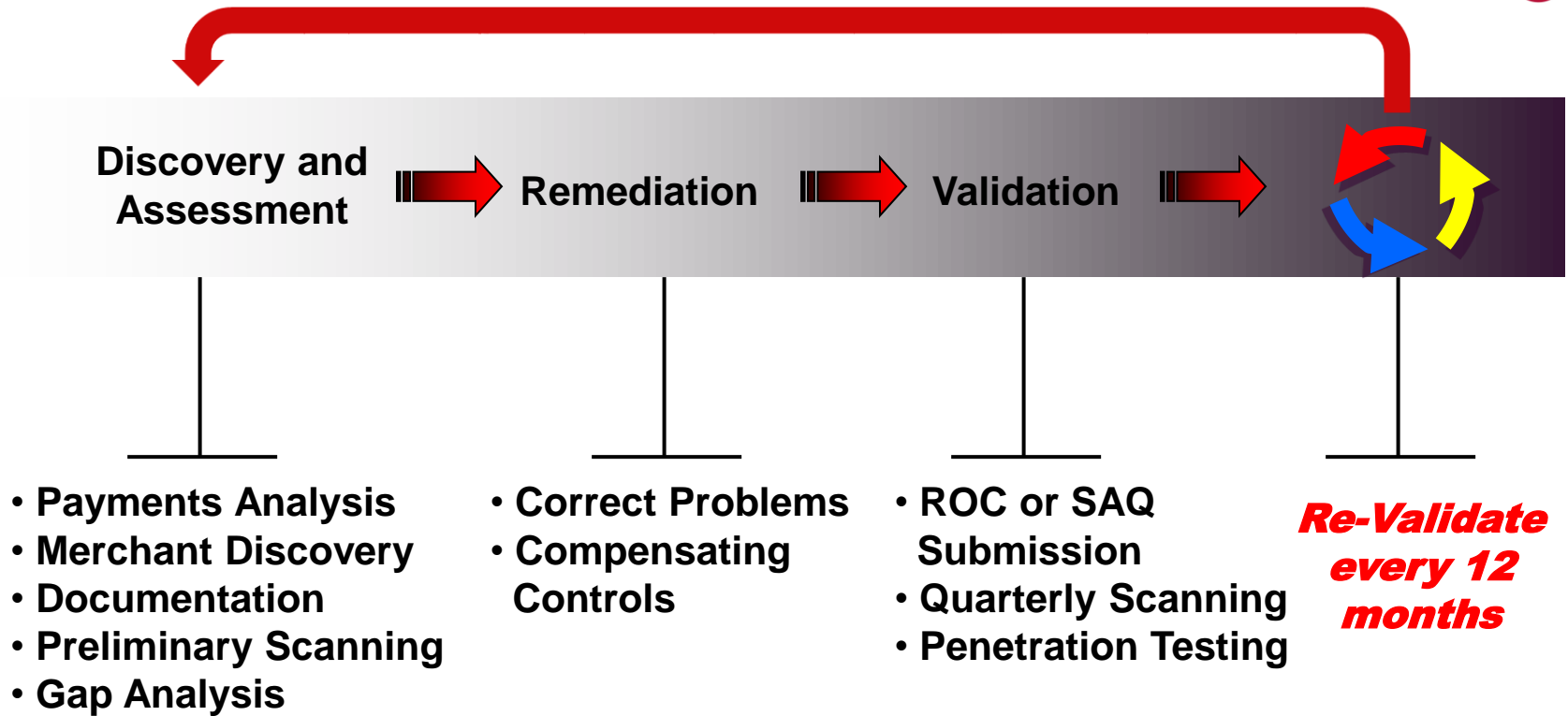
- Sonic Drive-In
- Lord & Taylor and Saks Fifth Avenue
- Orbitz
- The Buckle
- Arby's
- Cici's
- Omni Hotels & Resorts
- Wendy's
- Noodle's and Company
- Hyatt
- Trump Hotels
- Hilton Hotels
- Starwood (Marriott)

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 is a Process



Resources



- PCI Security Standards Council
 - www.pcisecuritystandards.org/
- Card Brands
 - www.visa.com/cisp
 - www.mastercard.com/sdp
 - <https://www.discoverglobalnetwork.com/solutions/pci-compliance/discover-information-security-compliance/>
 - <https://www.americanexpress.com/us/merchant/us-data-security.html>
- DBIR
 - <https://www.verizon.com/business/resources/reports/dbir/>
- KrebsOnSecurity
 - <http://www.krebsonsecurity.com/>
- CampusGuard
 - www.campusguard.com/



Jarvis Gilmore, CISSP, QSA
Security Advisor
CampusGuard
+1.832.598.1475
jgilmore@campusguard.com