



VECTRA
CORPORATION

••• PCI DSS Overview

Computer Security Day 2007

Lyal Collins

12/1/2007 11:43 AM



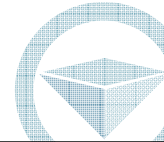
Outline

- PCI background and timeline
- To whom does PCI apply?
- Overview of PCI requirements
- Related standards; PCI PED, PABP/PA DSS
- Recent PCI announcements
- Things we have seen in the field
- The future of PCI



❖❖ Background

- Credit card compromises are occurring globally and are increasing
- Financial and brand damage main risk to merchants
- Pre 2000, unique security standards and requirements for Merchants and Service Providers
 - Messy, confusing
- The birth of PCI Data Security Standard = Version 1.0
 - Major schemes amalgamated their standards in 2005
- The standard continues to evolve
 - Sept 2006 - PCI DSS V1.1
 - Released by the PCI Security Standards Council
 - No longer Card Brand specific
- Brands maintain their own program of
 - Validation requirements
 - Compliance reporting and tracking etc
- Industry self regulation



❖❖ Some Terms You'll Hear Today

- Payment Card Industry Security Standards Council
 - PCI SSC, PCI Council
- QSA
 - Qualified Security Assessor
 - Trained and Qualified by PCI SSC to perform PCI audits
 - **QSAC** = QSA Company, e.g. my employer
- ASV
 - Accredited Scanning Vendor
 - Accredited by PCI SSC to perform vulnerability scanning to a minimum criteria
- Acquirer
 - Maintains merchant's account for credit card payments
- Issuer
 - Maintains cardholder's credit card account
- Brand, Scheme
 - E.g. Visa, MasterCard, American Express, JCB, Diners



Who must comply with PCI DSS

Any entity who

- “processes, stores or transmits cardholder information”

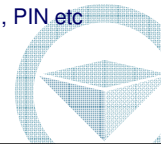
Scope* includes:

- ...all “system components.”
- “A system component is defined as any network component, server, or application that is included in or connected to the cardholder data environment.”
- “cardholder data environment is that part of the environment that processes, stores or transmits cardholder information or sensitive authentication data”

“Cardholder information” includes:

- Card account number (also called PAN, Primary Account Number)
- Card verification/authentication codes e.g. CVC2, CV2, CID, PIN etc
- Name, expiry date etc when in conjunction with the PAN

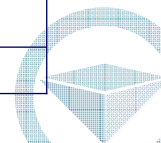
* See “PCI DSS Security Audit Procedures”, page 5



Merchant Compliance Levels

Despite there being a common standard, each scheme has its own compliance program

Level	MasterCard	Visa
1	> 6 million MasterCard transactions by any channel, or compromised merchants	> 6 million Visa transactions by any channel, or compromised merchants
2	> 150,000 MasterCard ecommerce transactions, or 1-6 million transactions via any channel	1-6 million transactions via any channel
3	> 20,000 MasterCard ecommerce transactions	20,000 – 1 million Visa ecommerce transactions
4	All others	All others



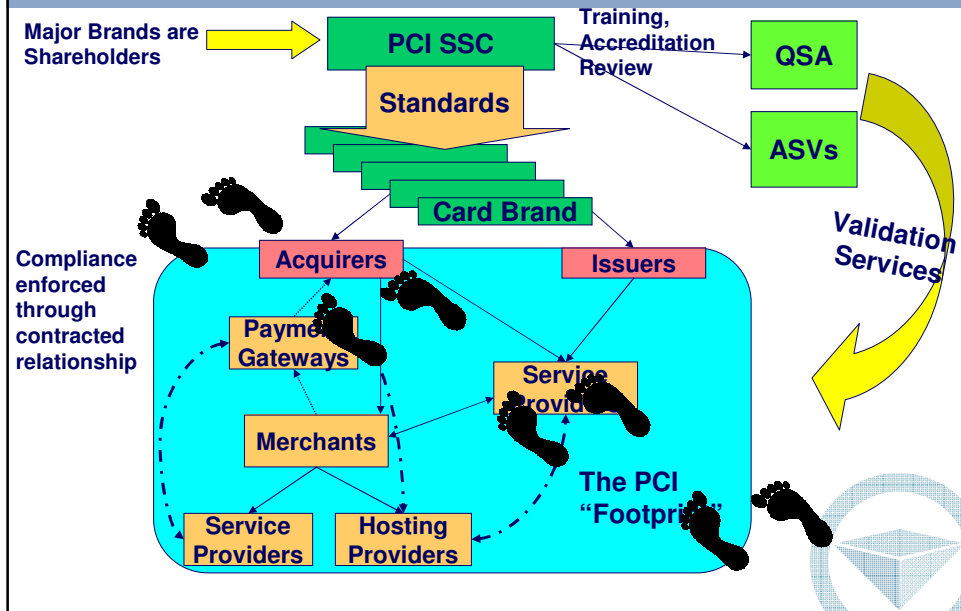
❖❖ Merchant Compliance Validation

Level	Validation Action	Validated By
1	Annual On-site PCI Data Security Assessment	Qualified Security Assessor Company Internal Audit if signed by Officer of the Company
	Quarterly Network Scan	Approved Scanning Vendor
2	Annual PCI Self-Assessment Questionnaire	Merchant. Optional: On-site review
	Quarterly Network Scan	Approved Scanning Vendor
3	Annual PCI Self-Assessment Questionnaire	Merchant.
	Quarterly Network Scan	Approved Scanning Vendor
4	Annual PCI Self-Assessment Questionnaire	Merchant.
	Quarterly Network Scan	Approved Scanning Vendor (where relevant) Validation is optional (MasterCard Only)

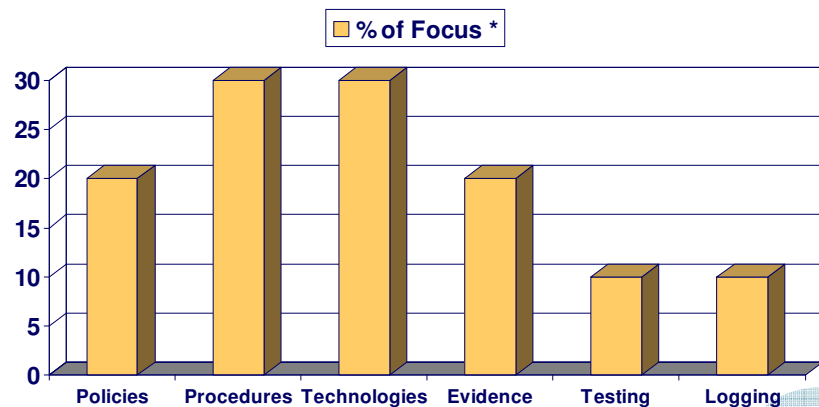
❖❖ Examples of entities in scope of PCI – i.e.

- Merchants = accept payment
- Service Providers = assist with payment or cardholder support
 - Third Party Processors
 - Hosting Providers
 - Software Developers
 - Outsourcers
 - Loyalty programs
 - Aggregators
 - Payment Gateways
 - Data Storage Entities
 - Card manufacturers
 - Billing services
- Issuers = manage cardholder accounts, manufacture and distribute cards

Who's Who in the PCI 'zoo'



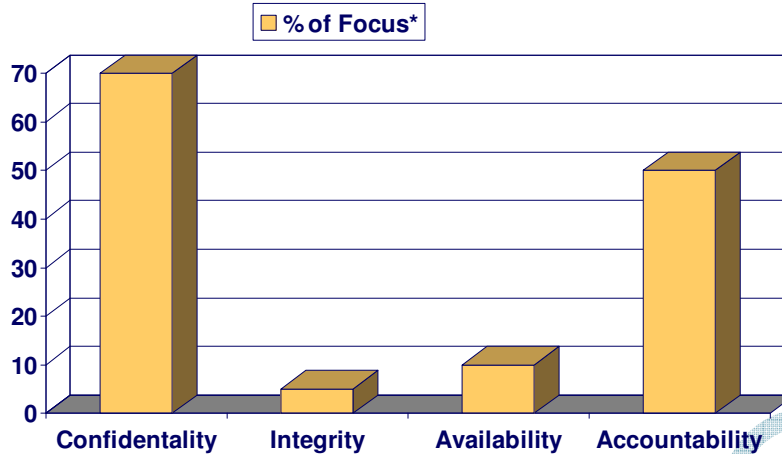
Requirements By Focus Area



* Note – approximations of "relevance"

Requirements vs. Security Primitives

Its about card data confidentiality and who did what, when !



* Note – approximations of “relevance”

Summary of Data Protection Requirements

	Data Element	Storage Permitted	Protection Required	PCI DSS Reqt 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes*	Yes
	Cardholder Name	Yes	Yes*	No
	Service Code	Yes	Yes*	No
	Expiration Date	Yes	Yes*	No
Sensitive Authentication Data **	Full Magnetic Stripe	No	N/A	N/A
	CVC2	No	N/A	N/A
	PIN, PIN Block	No	N/A	N/A

* Subject to other legislation requirements, must be protected if stored with PAN

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

Merchant Compliance Reporting

Reporting Responsibilities

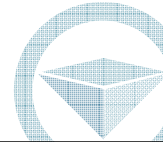
Level	MasterCard	Visa
1	Annually: Acquirer <u>must</u> register compliant merchants Quarterly: Report status of non-compliant merchants	Certificate of Compliance (submitted by Acquirer) if merchant is compliant
2	As above	Acquirer manages compliance No reporting to Visa
3	As above	Acquirer manages compliance No reporting to Visa
4	Annually: Acquirer <u>may</u> register compliant merchants	As above

The Five “Toos” We Commonly Find

“Too”	Activity or process
Much	<ul style="list-style-type: none"> ▪ Retained card data ▪ Complacency
Little	<ul style="list-style-type: none"> ▪ Storage protection ▪ Awareness ▪ Documentation: - Policies, Procedures, Change Management ▪ Logging and auditing capabilities
Long	<ul style="list-style-type: none"> ▪ Retention period for PANs/Track 2
Short	<ul style="list-style-type: none"> ▪ Retention of Logs, CCTV records etc
Infrequent	<ul style="list-style-type: none"> ▪ Reviewing of logs and audit trails ▪ Testing: - Pen tests, Vulnerability scanning, Development ▪ Incident Response planning and review ▪ Policy reviews and updates

❖❖ Payment Application Best Practices (PABP)

- Visa 'recommended' standard
- Mandated from Jan 1, 2008 in USA
 - Asia Pacific – watch this space!
- Third party card processing software
- Simplifies PCI audits
 - Ensures third party products observe the authentication, storage, logging, development and patching requirements of PCI
- Minimises security breaches from poor designs and implementations
- ~ 100 applications have already been accredited by Visa
 - More to come
- PCI SSC intend to release PA-DSS in H1, 2008



❖❖ PCI Next Steps

- PCI Compliance Reporting
 - December 2007 – existing entities
 - December 2008 – new entities
- PABP/PA-DSS is coming
 - Expectation is 2008 for Asia Pacific
 - Will become PA DSS in 2008, under PCI Council
 - 2010: end of life for non-complaint apps
- Updated PCI requirements (Version 1.2?)
 - Potentially, Q3 2008
- More entities being fined
- Fines and other penalties will increase
 - Dollar values
 - Enforcement of compliance





V E C T R A
C O R P O R A T I O N



Thank you

Questions ?

12/1/2007 11:43 AM