Achieving and Maintaining PCI Compliance

Nelson Brito
Senior Security Engineer
nbrito@br.ibm.com

innovation that matters

AGENDA

- What are the Facts
- What is PCI DSS?
- Importance to Business Leaders
- Debunking Myths and Solving Sticky Points
- PCI Compliance Solutions

The QSA View of the PCI DSS Compliance World

- **If all the Merchants, Service Providers, Issuers, Acquirers, and Payment Gateways viewed cardholder data as Nuclear Toxic Waste they would limit**
  - The number of places that glow in the dark
  - The number of individuals that glow in the dark
  - Prevent anyone not absolutely needed to glow in the dark to be quarantined from this data

PCI in the News

- **International Retail Organization victim to largest payment card heist in history**
  - **94 million card numbers stolen**
  - **Up to $1B (USD) in costs anticipated**
  - **Fraud & Lawsuits**
- **Recent Payment Card Data Breaches:**
  - **Global Entertainment Company - Insider**
  - **West Coast University – Insider**
  - **Professional Sports Association – External**
- **Recent Local Breaches:**
  - **September08: Stolen credit card information in the UAE** which was then used to make fraudulent purchases in the US.
  - **September08: Fraudulent money withdrawals.** Lloyds TSB, Emirates NBD, HSBC, Citibank, National Bank of Abu Dhabi and Dubai Bank affected.
  - **October08: More ATM card fraud in UAE and Qatar.** Qatar Islamic Bank and HSBC in Doha affected, Standard Chartered Bank in Dubai.
  - **Novembe08: More ATM card fraud in UAE. A gang of four men were arrested, accused of a $60 million fraud operation involving stolen credit card information.**
- **60% of Frauds today are Credit Card Frauds** (***Source: Fraud information is from PCI Town Meeting 22 October 2008)***

Who is to Blame for the Losses view from the PCI DSS Requirements

- **Risky Behavior by Merchants, Service Providers, Acquires, and Issuers**
  - 81% store the Primary Account Number (PAN) – You know this as the card number
  - 73% store the expiration date - Note when stored with PAN this is to be protected the same as the PAN
  - 53% store all or portions of the magnetic strip data – Note full track data is prohibited data as is the CVV, CVC, or CVS data
  - 16% store privacy and personal data

Source: PCI Town Meeting Brussels 22 October 2008

Who is to Blame for the Losses view from the Consumers Perspective

Would you believe that you fit one of the following knowing we are all consumers

- 21% blame the Consumer - themselves
- 21% blame the Card Brands
- 19% blame the retail merchants
- 14% blame the Issuer
- 13% do not who to blame

Source: PCI Town Meeting Brussels 22 October 2008

View of the Problem from the Cyber Crime Perspective

- **Cyber Crime for which Credit Card Fraud fall under is approaching the size and intensity of the Illegal Drug trade.**
  - International Law enforcement anticipate this financial crime will surpass the drug trade in the next three years
    - Volume of dollars gained illegally
    - Impact on the world economy
  - The majority of these crimes are from the inside in part by the use of
    - Social engineering
    - Phishing – a form of social engineering
    - Application breaches due to poorly written applications

Source:

PCI Town Meeting Brussels 22 October 2008 – Europol and Interpol
Peter Zinn Netherlands Police Agency
PCI SSC PA-DSS Training July 2008

What is PCI DSS?

- **Payment Card Industry Data Security Standard (PCI DSS) is a global security program that was created to increase confidence in the payment card industry and reduce risks to PCI Members, Merchants, Service Providers and Consumers.**
- **Current Version is PCI DSS 1.2 released the first of October 2008**
- **PCI SSC has the Following Global Requirements**
  - PCI-DSS
  - PA-DSS
  - ASV
  - PID and POS

Who does PCI DSS apply to?

- **All merchants & service providers that <u>store, process or transmit cardholder data</u>**

- **Applies to:**
  - **Retail** (online & brick & mortar)
  - **Hospitality** (restaurants, hotel chains, etc.)
  - **Transportation** (i.e. airlines, car rental, etc.)
  - **Financial Services** (banks, credit card processors, brokerages, insurance companies, etc.)
  - **Healthcare/Education** (hospitals, universities)
  - **Government** (where payment cards are accepted)
  - **Service Providers** (where they can impact the card data)
  - **Application Vendors** (where the application are used for cardholder data processing)
  - **POS and PID Suppliers**

PCI DSS Requirements

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

PCI DSS Ver. 1.1

The Standard vs. Enforcement

- **In September 2006, the major payment card providers created the PCI Security Standards Council (PCI SSC)**
  - Visa
  - MasterCard
  - American Express
  - Discover
  - JCB
- **PCI SSC is an independent body to govern the global security standards for the payment card industry**
- **The individual card companies (Visa/MC) are responsible for validating/enforcing compliance against PCI DSS**

The Five Myths of PCI Compliance

- PCI Compliance is Hard and no one is doing it!
- PCI will make the company secure!
- Encryption is scary and very difficult!
- I do not process enough Payment Cards to Worry about PCI
- There is a tool that will make me Compliant!

PCI Compliance Sticking Points

Common Issues/Challenges:

- Lack of knowledge as to where cardholder data is located
- Storage of prohibited cardholder data
- Lack of a network segmentation
- Use of production cardholder data in test environments
- Lack of proper encryption
- Lack of Logging and Log review

Data Retention

- **Post authorization you are not permitted to retain in any format**
  - Full Track Data
  - PIN Block Data
  - CVV type Data
- **Primary Account Number (PAN), also known as the full card number, must be encrypted or protected so that is not readable by anyone without a direct business need**

Are governments agencies exempt?

- **NO PCI applies to all**
  - NO all entities that process or use credit card data are under the same compliance
- **Can a government agency reach compliance with items marked as not in Place?**
  - NO The PCI DSS Compliance is a required 100% compliance
- **Can a government agency work with their acquirer to work toward compliance?**
  - YES in most cases

Non-Compliance Consequences

- **If non-compliant and a breach occurs…**
  - ***Merchants/Service Providers have liability for the acquirer bank's losses and card re-issuance costs***
  - Restrictions imposed by card companies (prohibiting future credit card processing)
  - Investigative and Legal costs
  - Repayment of losses may exceed the ability to pay and cause **total failure of the organization**

- **Other potential consequences:**
  - Damaged Brand Reputation
  - Negative Publicity
  - Loss of customers

VISA: Fines

- **Visa USA: Monthly Non Compliance Fines**
  - Acquirer banks will be fined $25k (USD) a month for each of its Level 1 and 2 merchants who have not validated by September 30, 2007 and December 31, 2007 respectively.
  - Acquirer banks failing to provide confirmation that their Level 1 and 2 merchants are not storing prohibited data, full track, CVV or PIN data by March 31, 2007 can be fined up to $25k a month per merchant and can have their interchange rate raised.

- **Visa Europe: Breach Fines**
  - Penalty schedule based upon number of account numbers compromised:
    - 1-19,999 25,000 Euros
    - 200,000-299,999 300,000 Euros
    - >500,000 750,000 Euros

Breach Costs

- **According to the five PCI Card Brands a Breach Cost the Company**
  - 60 to 200 times the cost of Compliance
- **Compliance cost approximately $3.00 USD per card in the systems**
- **Breach cost approximately $300 USD per card for each card in the systems.**
  - Example the company has 2,000 cards in the systems and 50 are breached
    - Breach cost are estimated at $600,000 USD.

Benefits of Compliance

Compliance Benefits	
Everyone	• Reduce risk • Increase confidence in payment industry • ***Safe Harbor Protection***
Members	• Protect reputation
Merchants and Service Providers	• Gain competitive edge • Increase revenue and improve bottom line • Maintain positive image • Protect customers
Industry	• Encourage “good security neighbors” • Complies with the EU Privacy Requirements
Consumers	• Safeguarding of information • Prevention of identity theft

Source: Visa USA

Our Proprietary Methodology To Assist You in PCI Compliance

- **IBM performs an assessment NOT an Audit. We work "hand in hand" to partner with you and your company to achieve compliance**
- **Our methodology focuses on understanding your unique role with payment card data, associated business risk and processes in correlation with the PCI standards.**
- **Our goal is to produce a roadmap which will enable you not only to be compliant, but to reduce the risk to cardholder data**
- **IBM ISS conducts a PCI Gap-Assessment (iRoc)**
  - If PCI deadline is near, ISS will work with Acquiring Banks or Card Companies to let them know the testing is in progress
- **Based on assessment results, IBM ISS works with client to develop a remediation plan to close gaps**
  - Policy development
  - Compensating controls
  - Network architecture design
- **Formal PCI ROC assessment conducted after all remediation's performed**
  - ISS performs hands-on validation and technical testing
  - Final "clean" assessment report delivered for compliance

IBM ISS Helping Clients Achieve PCI Compliance

- Compliance requirements vary by type of organization (Merchant vs. Service Provider) and also based on payment card transaction volume
- **Internet Security Systems (ISS), a wholly owned IBM Company, is "Globally Certified" to perform PCI services**
  - IBM ISS is a "Qualified Security Assessor" per PCI SSC
  - Individual consultants must be trained yearly for various PCI certifications
- ISS QSA PCI Services:

1. PCI Gap-Assessment (iRoc) Consulting
2. PCI On-Site Annual ROC Assessment
3. PCI Quarterly Network Scanning
4. PCI Payment Application Assessments
5. PCI Subject Matter Expertise
6. PCI Incident Response Services

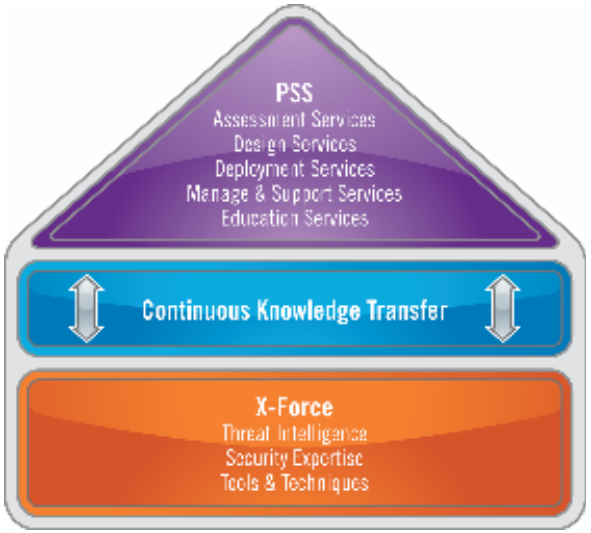
- Additional IBM PCI Services:

1. PCI Remediation Planning
2. PCI Remediation Project Management
3. PCI Remediation Project Staffing
4. PCI Penetration Testing

IBM PCI Differentiators

- ***IBM Internet Security Systems is PCI Services Market Leader***

FROST & SULLIVAN



- **IBM ISS is "Globally Certified" to perform PCI services**
  - Qualified Security Assessor (QSA)
  - Approved Scanning Vendor (ASV)
  - Qualified Payment Application Security Company (QPASC)
  - Qualified Incident Response Company (QIRC)
- **IBM ISS Methodology – Assessing not Auditing**
  - Performing a gap assessment upfront
  - Providing specific recommendations for becoming compliant
  - Working with client to help them achieve compliance
- **Security Expertise**
  - Deep expertise performing security assessments
  - Understanding of vulnerabilities and attack methods
  - X-Force security intelligence
- **Incident Response**
  - As a Qualified Incident Response Company, IBM ISS can assist organizations with security incidents involving payment card data
  - Able to provide incident response planning to merchants and service providers in advance of a security incident

IBM Services, Software and Hardware for Total PCI Compliance

Meeting Requirements of the PCI DSS Digital Dozen

The products outlined in this chart highlight IBM capabilities. Please call your local IBM executive for a full listing of all products and services that map to PCI requirements

IBM PROFESSIONAL SERVICES

IBM SOFTWARE SOLUTIONS

IBM MANAGED SERVICES

IBM HARDWARE

11 TEST SECURITY SYSTEMS AND PROCESS

- IBM ISS Products & Services
- Tivoli Security Compliance Manager
- IBM Proventia Network Anomaly Detection System (ADS)
- IBM Global Services
- IBM Rational AppScan

12 SECURITY POLICY FOR EMPLOYEES & CONTRACTORS

- IBM Global Services
- Tivoli Console Insight Manager

1 FIREWALL TO PROTECT CARDHOLDER DATA

- IBM Proventia Server Intrusion Prevention System (IPS)
- IBM Proventia Network (IPS)
- IBM Global Services

10 MONITOR ACCESS

- IBM Tivoli Compliance Insight Manager
- IBM Tivoli Security Operations Manager
- IBM Proventia Server IPS
- IBM Global Services

2 NO DEFAULT PASSWORDS OR SECURITY PARAMETERS

- IBM Tivoli Access Manager
- IBM Proventia Network Multi-Function Security

SECURE & PROTECT CARDHOLDER DATA

9 RESTRICT PHYSICAL ACCESS

- IBM Digital Video Surveillance
- IBM Biometric Access Control
- IBM Global Services

3 PROTECT STORED CARDHOLDER DATA

- IBM Storage Manager
- IBM Proventia Server IPS
- IBM PKI Services
- IBM Global Services

8 UNIQUE IDs

- IBM Tivoli Identity Manager
- IBM Tivoli Federated Identity Manager
- IBM Global Services

4 ENCRYPT TRANSMISSION

- IBM Data Encryption of IMS and DB2
- IBM Websphere
- Proventia Network Intrusion Prevention System

6 SECURE SYSTEMS & APPLICATIONS

- IBM Software Development Platform
- IBM Tivoli CCMBD
- IBM Global Services
- IBM Rational AppScan

7 RESTRICT ACCESS

- IBM Tivoli Access Manager
- IBM Tivoli zSecure Admin
- IBM Tivoli Compliance Insight Manager
- IBM Global Services

5 USE & UPDATE ANTI-VIRUS SOFTWARE

- IBM Proventia Desktop Endpoint Security
- IBM Proventia Network Enterprise Scanner
- IBM Global Services

Merchants – Level Criteria

Merchant Level	Criteria
Level 1	▪ 6 Million or more credit card transactions per year ▪ Merchants successfully compromised in the past year
Level 2	▪ 1 million to 6 million credit card transactions per year
Level 3	▪ 20,000 to 1 million e-commerce transactions per year
Level 4	▪ Less than 20,000 e-commerce transactions per year ▪ All other merchants processing up to 1 million credit card transactions per year

Compliance Requirements for Merchants

Validation Priority	Validation Action Required	Scope of Validation	Validation Actions:
Level 1	▪ Annual On-site Review (Report On Compliance) ▪ Quarterly System Perimeter Scan	▪ Authorization & Settlement Systems ▪ Internet Facing Perimeter Systems	▪ Independent Assessor or Internal Audit if signed by Officer of the company
Level 2	▪ Annual PCI Self-Assessment Questionnaire ▪ Quarterly System Perimeter Scan	▪ Internet Facing Perimeter Systems ▪ Any systems storing, processing, or transmitting Visa cardholder data	▪ Qualified Independent Security Assessor ▪ Merchant
Level 3	▪ Annual PCI Self-Assessment Questionnaire ▪ Quarterly System Perimeter Scan	▪ Internet Facing Perimeter Systems ▪ Any systems storing, processing, or transmitting Visa cardholder data	▪ Qualified Independent Security Assessor ▪ Merchant
Level 4	▪ Annual PCI Self-Assessment Questionnaire ▪ Quarterly System Perimeter Scan	▪ Internet Facing Perimeter Systems ▪ Any systems storing, processing, or transmitting Visa cardholder data	▪ Qualified Independent Scan Vendor ▪ Merchant

Thank You

Nelson Brito
Senior Security Engineer
nbrito@br.ibm.com

innovation that matters