



ISACA Vancouver Chapter  
PCI Presentation  
Tuesday November 10<sup>th</sup>, 2009



# Agenda

- Data Breach Stats – Why did PCI DSS come about
- PCI Council – What is it
- What is the PCI DSS, and who must comply with it
- PCI Scope / Network Segmentation
- Compliance Requirements / Merchant Levels
- Penalties
- Path to Compliance

# Data Breach Statistics

## Who is behind data breaches?

- 73% resulted from external sources
- 18% were caused by insiders
- 39% implicated business partners
- 30% involved multiple parties

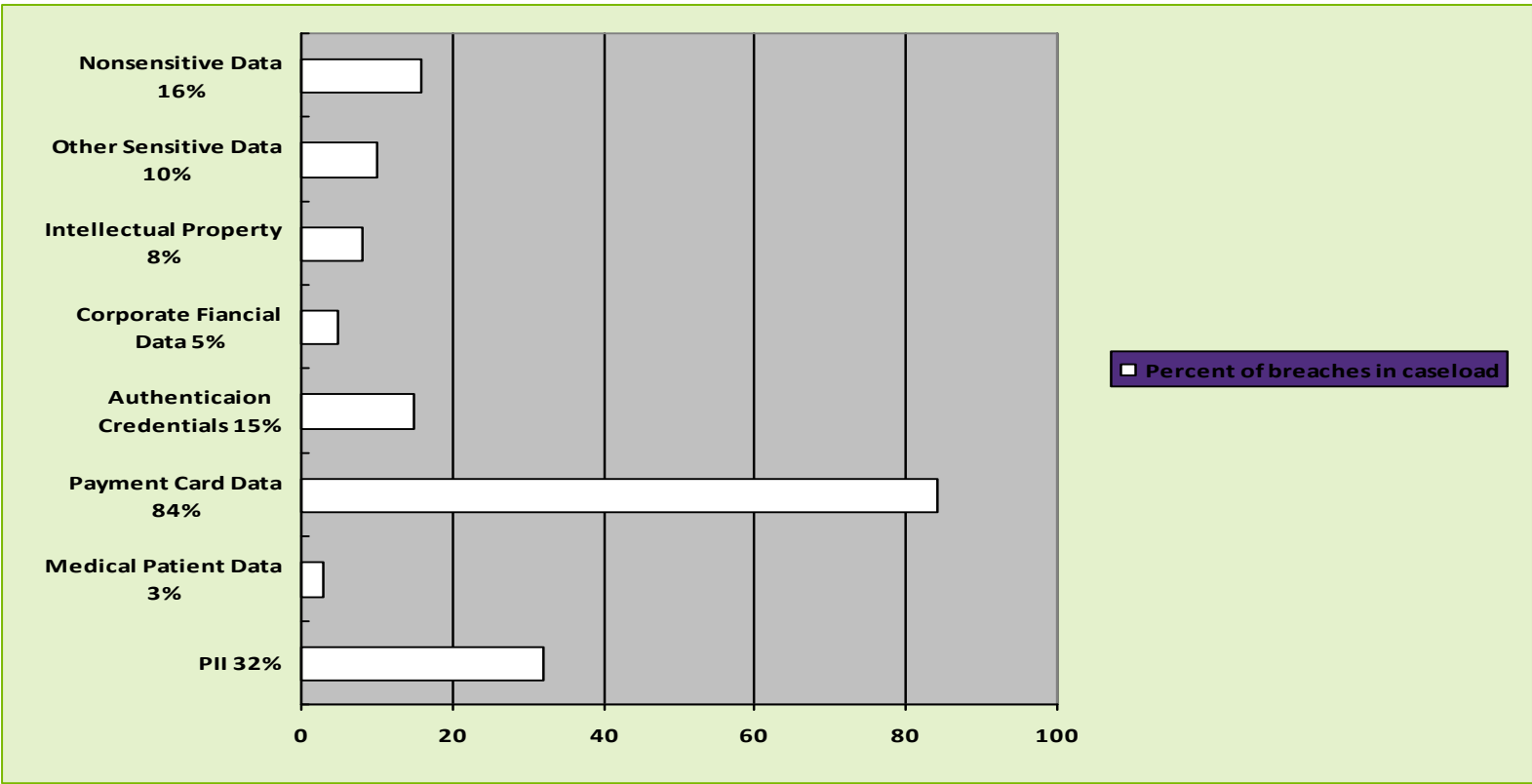
## What commonalities exist?

- 66% involved data the victim did not know was on the system
- 75% of breaches were not discovered by the victim
- 83% of attacks were not highly difficult
- 85% of breaches were the result of opportunistic attacks
- 87% were considered avoidable through reasonable controls

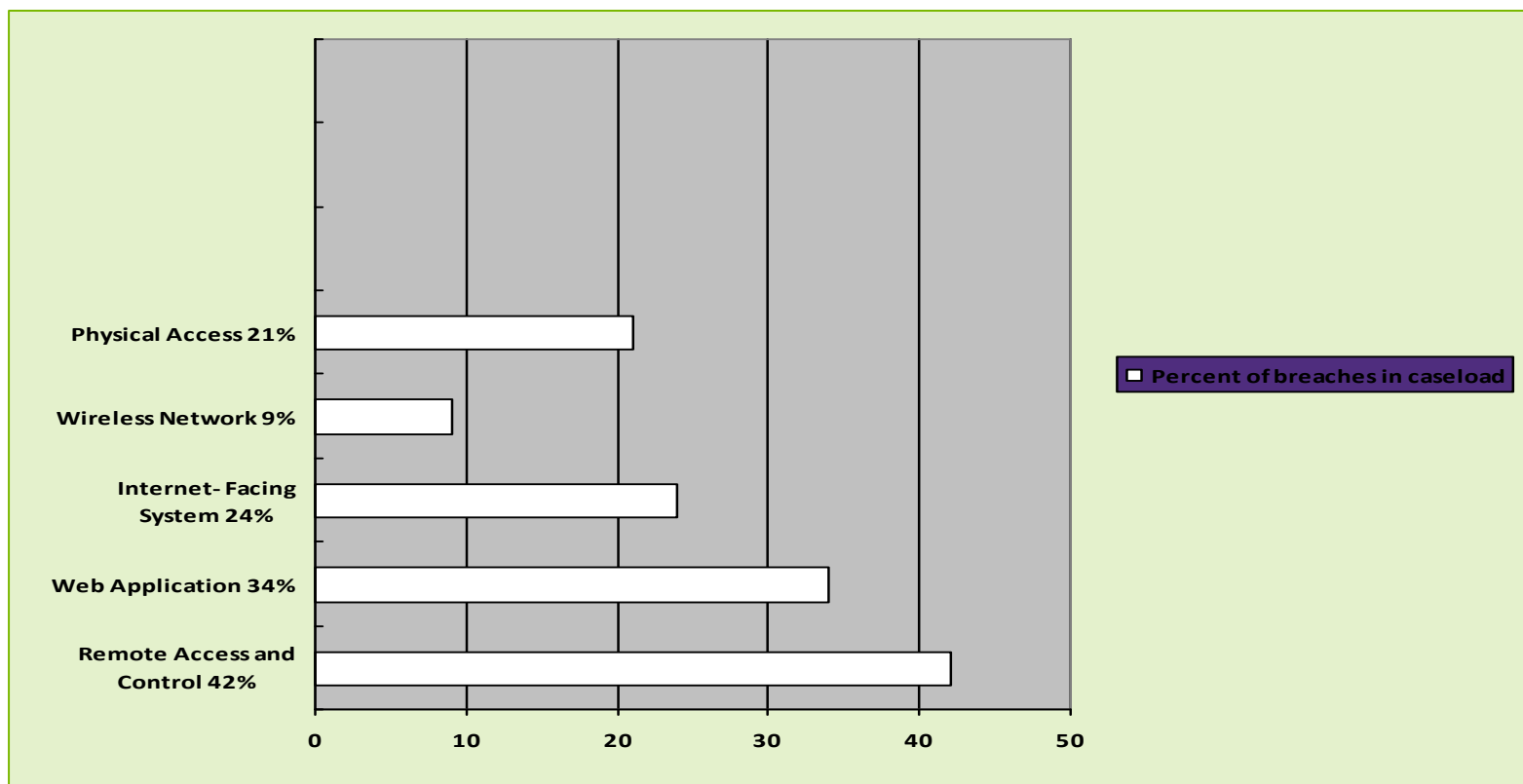
## How do breaches occur?

- 62% were attributed to a significant error
- 59% resulted from hacking and intrusions
- 31% incorporated malicious code
- 22% exploited vulnerability
- 15% were due to physical threats

# What was stolen?



# What was attacked?



# What is the PCI Security Council

## What is PCI SSC?

- An independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards on a global basis
- Founding multi-national acceptance brand members:



# PCI Security Standards Council Objectives

- Issue new standards and manage standards life cycle
- Enhance payment account security
- Create awareness and drive adoption of standards
- Foster participation and gather feedback
- Manage the qualification and approval testing process for ASVs/QSAs/PA-QSAs and PED Labs
- Maintain a current list of approved QSAs, ASVs, PA-QSAs, validated payment applications and PED approved devices

# PCI DSS- what is it?

- Payment Card Industry Data Security Standard
- Is a formalized security standard
- Covers security of the systems and networks that store, process and transmit card data
- Currently at version 1.2
- Revised on a 24 month cycle

# What does it cover?

Six major areas and twelve requirements to review:

## Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

## Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

## Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus information
6. Develop and maintain secure systems and applications

# What does it cover? (cont'd)

Six major areas and twelve requirements to review (cont'd)

## Implement Strong Access Control Measures

7. Restrict access to 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

# Who must comply?

## Who must comply?

- All members, merchants, and service providers that **store, process, OR transmit cardholder data**
- All system components which are defined as any network component, server, or application that is included in or connected to the cardholder data environment.
- So... it means merchants, mail order, phone order, payment processors, credit card processing, clearing, etc

# Service Providers

- A service provider is a business entity directly involved in the processing, storage, transmission, and switching of transaction data and cardholder data
  - Usually not a payment card brand member
  - Sometimes a service provider is a merchant
- Includes companies that provide services to merchants, service providers or members that control or could impact the security of cardholder data.

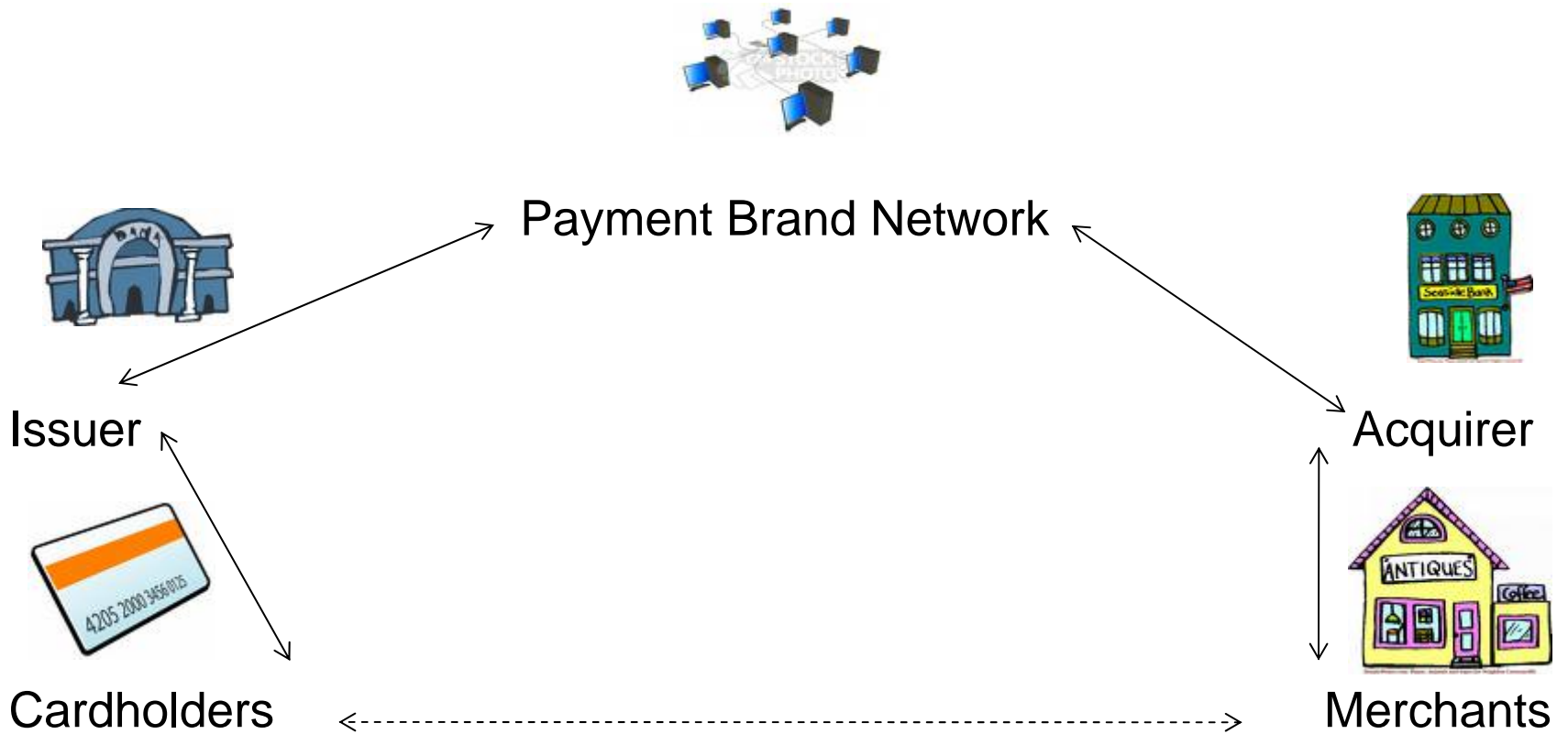
# Service Provider Examples

- **Transaction Processors**
  - Enables transactions such as authorization and settlement between merchants and issuers or acquirers.
- **Payment Gateways**
  - Enables transactions between merchants and processors
- **Independent Sales Organizations (ISOs) or External Sales Agents (ESAs)**
  - Perform cardholder and merchant program solicitations
- **Credit Reporting Services**
- **Customer Service Functions**

# Deadlines for Compliance

- Compliance is mandated by the payment card brands and not by the PCI Security Standards Council.
- However, for most merchants, the deadlines for validating compliance with the PCI DSS have already passed.
- In summary, all entities that transmit, process or store payment card data must be compliant with PCI DSS.

# Payment Industry Terminology



# Scope of PCI

The PCI DDS security requirements apply to all system components. 'System components' are defined as any network component, server, or application that is included in or connected to the cardholder data environment.

The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).

Applications include all purchased and custom applications, including internal and external (Internet) applications.

# What is cardholder data?

- Cardholder Data is the information printed on the physical card as well as the data on the magnetic strip or chip
- Cardholder Data includes:
  - Primary account number (PAN)
  - Cardholder name
  - Service Code
  - Expiration date
- Cardholder Data also includes Sensitive Authentication Data:
  - Magnetic Stripe or Track Data
  - Magnetic stripe image on a chip card
  - CAV2/CVC2/CVV2/CIID
  - PIN/ PIN Block
  - This data cannot be stored after authorization even if it is encrypted.

<b>Cardholder Data</b>	<b>Primary Account Number (PAN)</b>
	<b>Cardholder Name</b>
	<b>Service Code</b>
	<b>Expiration Date</b>
<b>Sensitive Authentication Data</b>	<b>Full Magnetic Stripe Data "Track Data"</b>
	<b>CAV2/CVC2/CVV2/CIID</b>
	<b>PIN/PIN Block</b>

# Cardholder Data Overview

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3,4
<b>Cardholder Data</b>	<b>Primary Account Number (PAN)</b>	YES	YES	YES
	<b>Cardholder Name</b>	YES	YES	NO
	<b>Service Code</b>	YES	YES	NO
	<b>Expiration Date</b>	YES	YES	NO
<b>Sensitive Authentication Data</b>	<b>Full Magnetic Stripe Data</b>	NO	N/A	N/A
	<b>CVC2/CVV2/CID/CA V2</b>	NO	N/A	N/A
	<b>PIN/ PIN Block</b>	NO	N/A	N/A

# Payment Brands Role

- All payment brands
  - Provide authorization & clearing/settlement services
  - Establish operating rules and regulations
  - Issue cards and acquire transactions through third parties (usually banks or credit unions)
- American Express, Discover, and JCB are also issuers and acquirers
- Visa and MasterCard do not issue cards or acquire transactions

# Payment Brand Compliance Programs

- Payment brands' compliance programs include:
  - Tracking and enforcement
  - Penalties, fees, compliance deadlines
  - Validation process and who needs to validate
  - Approval and posting of compliant entities
  - Definition of merchants and service provider levels
  - Forensic investigation for account data compromise
- Payment brands are also responsible for forensics and response to account data compromises

# Levels Matrix

## PCI compliance validation levels- merchant

	<b>Annual Visa Transaction Volume</b>	<b>Merchant Type</b>	<b>Self-Assessment Questionnaire</b>	<b>Vulnerability Scan</b>	<b>On-site Review</b>
1	Over 6,000,000	All Brick & Mortar MOTO eCommerce		Quarterly	Annual
2,3	20,000 to 6,000,000	eCommerce	Annual	Quarterly	
4A	1,000,000 to 6,000,000	Brick & Mortar MOTO	Annual	Quarterly	
4B	B/M and MOTO <1,000,000 eCommerce <20,000,000	All other merchants	Annual	Annual	

# Merchant Validation Requirements (Level 1 & 2)

Level	Amex	Discover	JCB	MasterCard	Visa
1	<ul style="list-style-type: none"> <li>-Annual onsite assessment by QSA or internal auditor if signed by officer of merchant company</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>-Annual onsite assessment by QSA or merchant's Internal Auditor</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>-Annual onsite assessment by QSA</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>-Annual onsite assessment by QSA or internal auditor if signed by officer of merchant company</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>-Annual onsite assessment by QSA</li> <li>- Quarterly network scan by ASV</li> <li>- Attestation of Compliance form</li> </ul>
2	<ul style="list-style-type: none"> <li><b>-EU Only:</b> Annual Self-Assessment Questionnaire</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>- Annual Self-Assessment Questionnaire</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>- Annual Self-Assessment Questionnaire</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>- Annual Self-Assessment Questionnaire</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>- Annual Self-Assessment Questionnaire</li> <li>- Quarterly network scan by ASV</li> <li>- Attestation of Compliance form</li> </ul>

# Merchant Validation Requirement (Levels 3 & 4)

Level	Amex	Discover	JCB	MasterCard	Visa
3	<ul style="list-style-type: none"> <li>-Quarterly network scan by ASV (recommended)</li> <li>- <b>EU Only:</b> SAQ (recommended)</li> </ul>	<ul style="list-style-type: none"> <li>-Annual Self- Assessment questionnaire</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>- N/A</li> <li>- N/A</li> </ul>	<ul style="list-style-type: none"> <li>-Annual Self- Assessment questionnaire</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>-Annual Self- Assessment questionnaire</li> <li>- Quarterly network scan by ASV</li> <li>- <b>Visa Europe:</b> Either complete annual SAQ and quarterly network scans OR use PCI DSS certified Payment Service Providers for all payment processing, storage and transmission</li> </ul>
4	<ul style="list-style-type: none"> <li>- N/A</li> </ul>	<ul style="list-style-type: none"> <li>-Compliance Validation requirements determined by acquirer. Recommended validation:</li> <li>-Annual Self- Assessment questionnaire</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>- N/A</li> </ul>	<ul style="list-style-type: none"> <li>-Compliance Validation is at discretion of acquirer</li> <li>To validate:</li> <li>-- Annual Self- Assessment questionnaire</li> <li>- Quarterly network scan by ASV</li> </ul>	<ul style="list-style-type: none"> <li>-Annual SAQ recommended</li> <li>- Quarterly network scan by ASV recommended</li> <li>- Compliance validation requirements set by acquirer</li> </ul>



# Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement.

Without adequate network segmentation (sometimes called a 'flat network') the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access to a particular segment of a network.

# Penalties and Fees for Non Compliance

## When do I get penalized?

- Not meeting PCI Compliance by the specified date.
- Card Holder data compromise when not PCI compliant

## What are the fines associated?

- Dependent on the card brand and acquiring bank
- Non- compliance (Visa Example)- \$5,000 and \$25,000 a month for each of its Level 1 and 2 merchants (Track data and CVV2 can be worse).
- Card Holder Breach (Visa Example)- Members are subject to fines, up to \$500,000 per incident, for any merchant or service provider that is compromised and not compliant at the time of the incident. Safe Harbour if PCI Compliant
- Impose restrictions on non- compliant merchants

# Other Costs of Non-compliance

## Outside of the card brands, what does Non-Compliance cost?

- 20% of individuals who received a data breach notification during 2005 terminated their relationship with that company
- Stock price: A 2004 study found that companies that suffered data breaches lost an average of just over 5% of their market valuation.
- Breach recovery: Average cost to recover from a data breach- \$14 million (\$140 per customer record)
  - Direct costs: \$50; Indirect costs: \$15; Opportunity costs: \$75
  - Average loss was 2.6% of all customers

# Path to Compliance

1. Determine the locations of the card holder data
2. Reduce scope by eliminating or segmenting the card holder data (electronic storage is automatically SAQ Validation Type 5)
3. Baseline your environment against the PCI DSS to identify gaps
4. For all gaps determine recommendations with associated effort (don't overlook "gotcha's" such as logging track data on a Point of Sales system).
5. Develop a prioritized plan to address gaps
6. Execute (... but with management support).