Deloitte.

Technical breakout session

Small leaks sink great ships – Managing data security, fraud and privacy risks

Tarlok Birdi, Deloitte

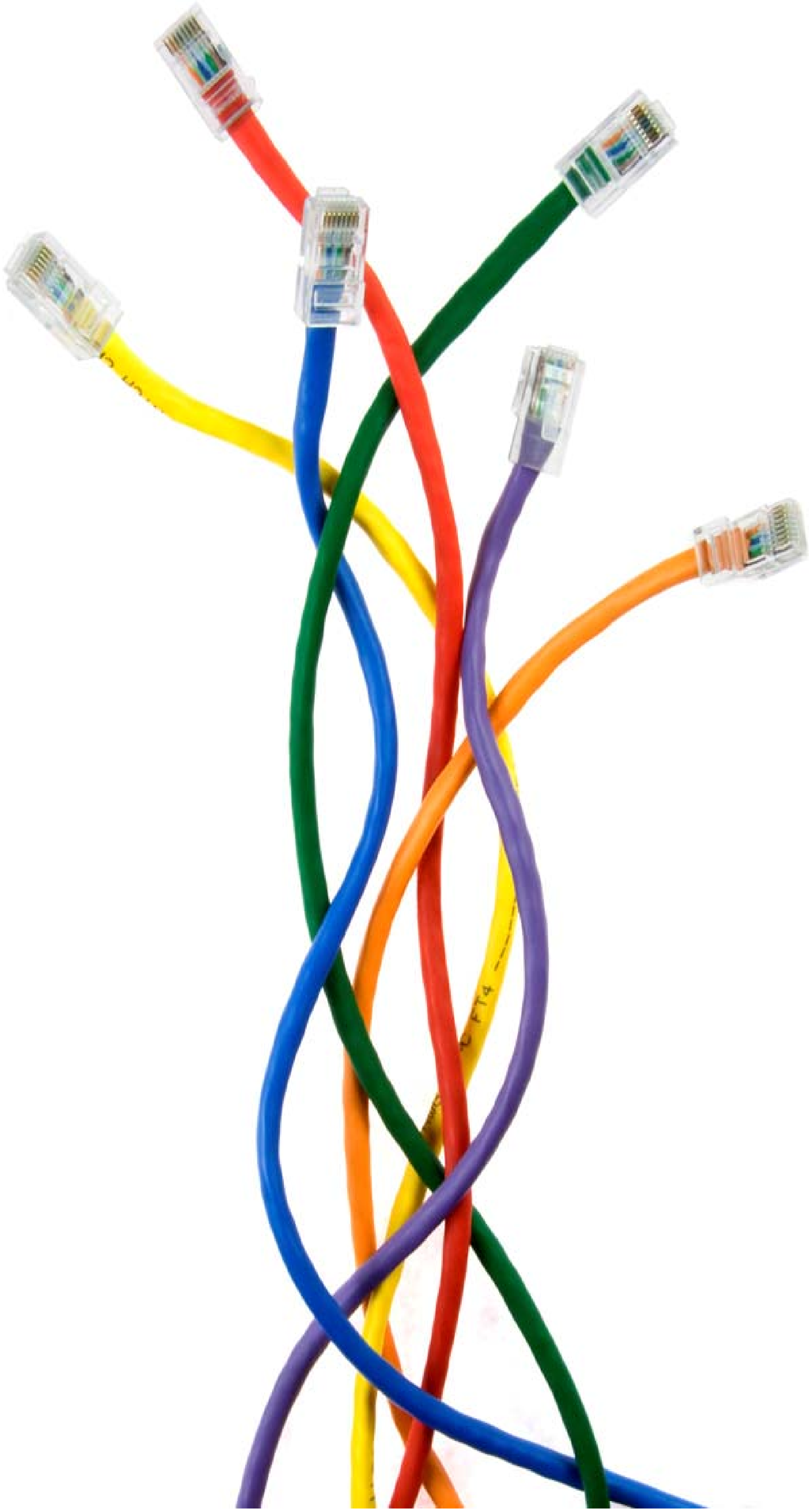
Ron Borsholm, WTS

May 27, 2009

Agenda

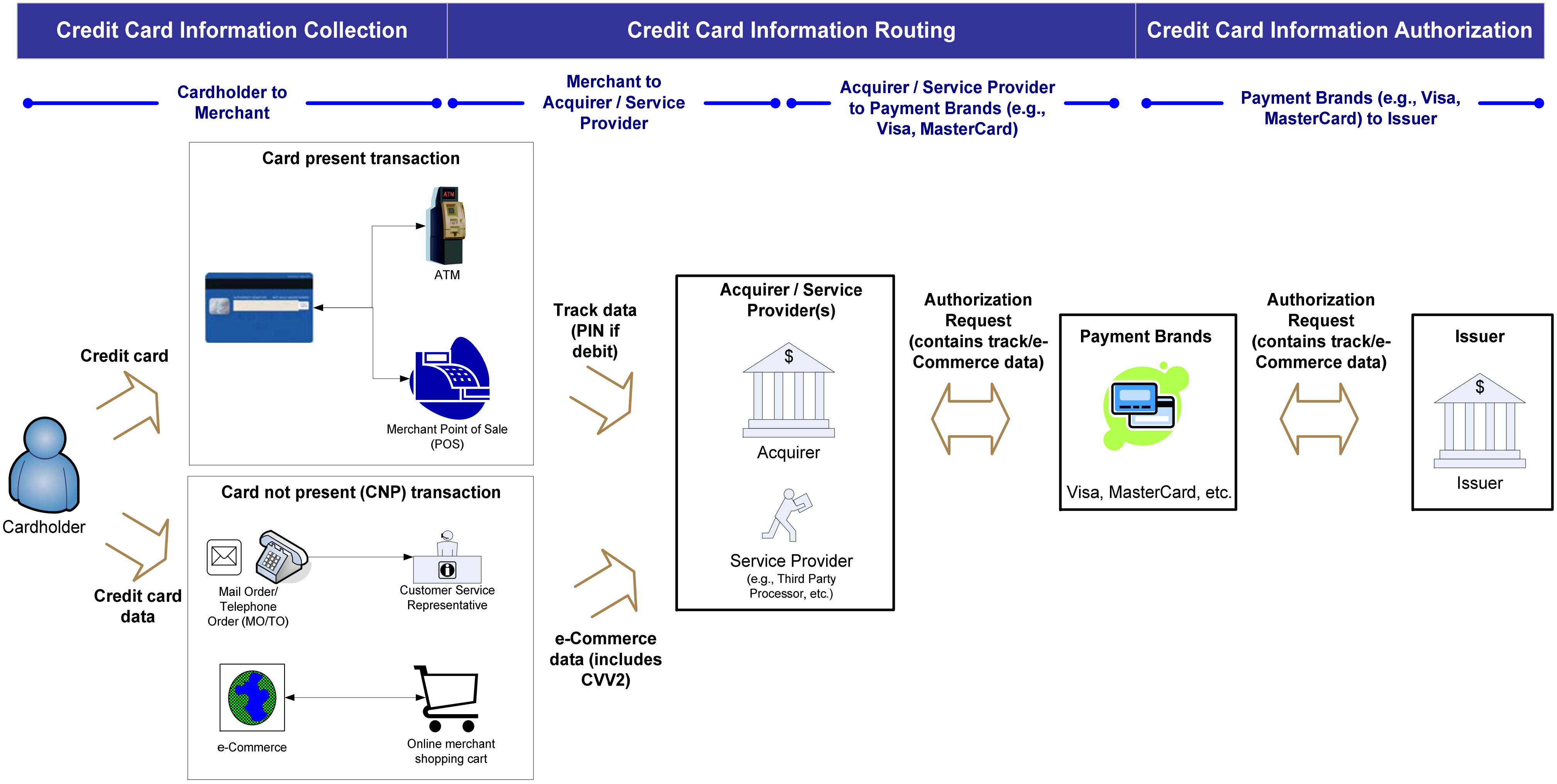
1. PCI overview: the technical intent
2. Scoping: what are the questions you should be asking
3. Roundtable discussion: what are your current challenges?
4. Common technical challenges and remediation approaches
5. Workplace Technology Services
6. Questions

PCI overview: the technical intent



Card flow primer

How does a transaction get processed?



Credit Card Information Collection

Credit Card Information Routing

Credit Card Information Authorization

Cardholder to Merchant

Merchant to Acquirer / Service Provider

Acquirer / Service Provider to Payment Brands (e.g., Visa, MasterCard)

Payment Brands (e.g., Visa, MasterCard) to Issuer

Cardholder

Credit card

Credit card data

Card present transaction

ATM

Merchant Point of Sale (POS)

Card not present (CNP) transaction

Mail Order/ Telephone Order (MO/TO)

Customer Service Representative

e-Commerce

Online merchant shopping cart

Track data (PIN if debit)

e-Commerce data (includes CVV2)

Acquirer / Service Provider(s)

Acquirer

Service Provider (e.g., Third Party Processor, etc.)

Authorization Request (contains track/e-Commerce data)

Payment Brands

Visa, MasterCard, etc.

Authorization Request (contains track/e-Commerce data)

Issuer

Issuer

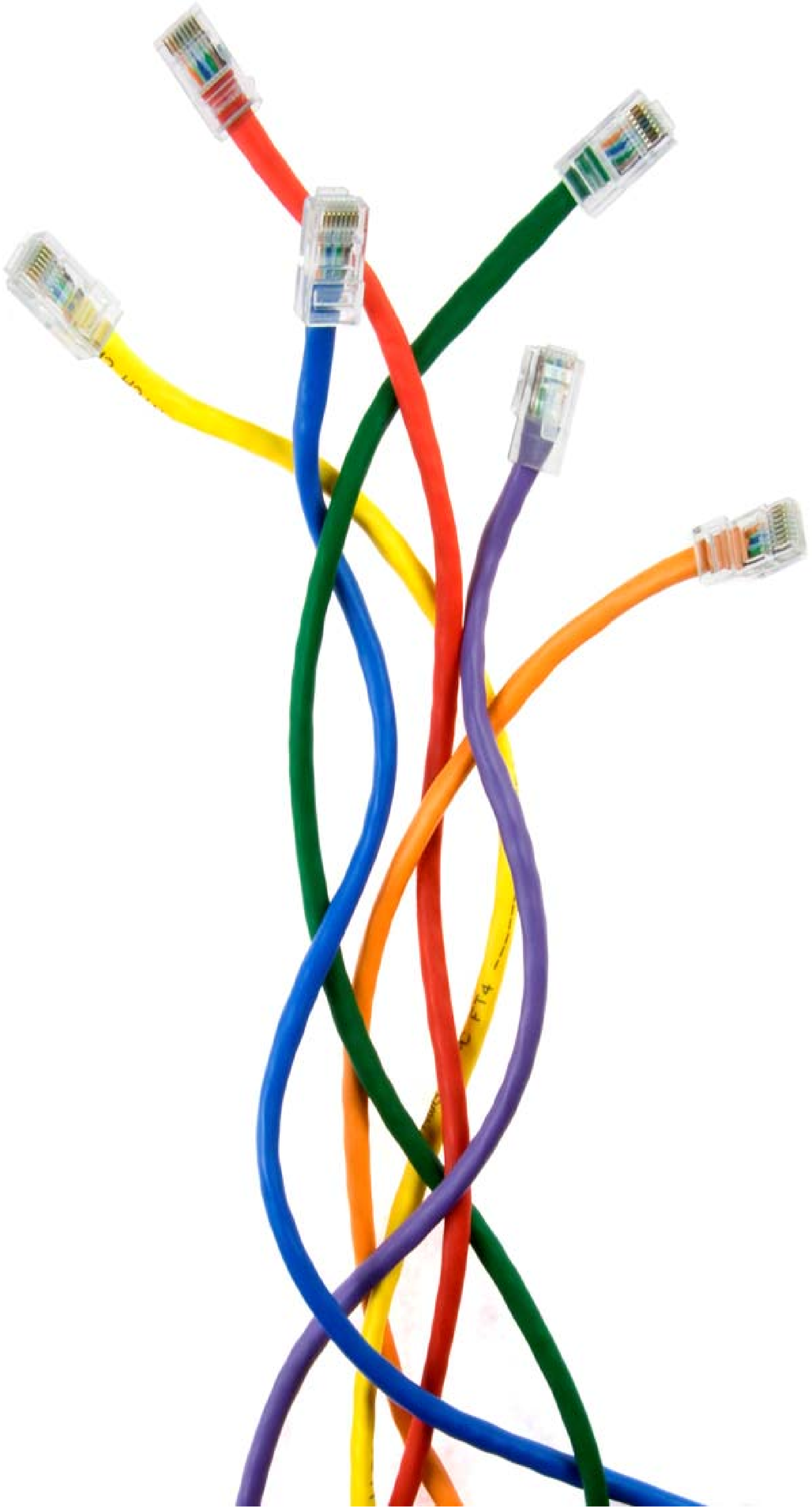
High level technical PCI requirements

PCI requirements
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-malware software 6 – Develop and maintain secure systems and applications

High level technical PCI requirements

PCI requirements
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

Scoping: what are the questions you should be asking?

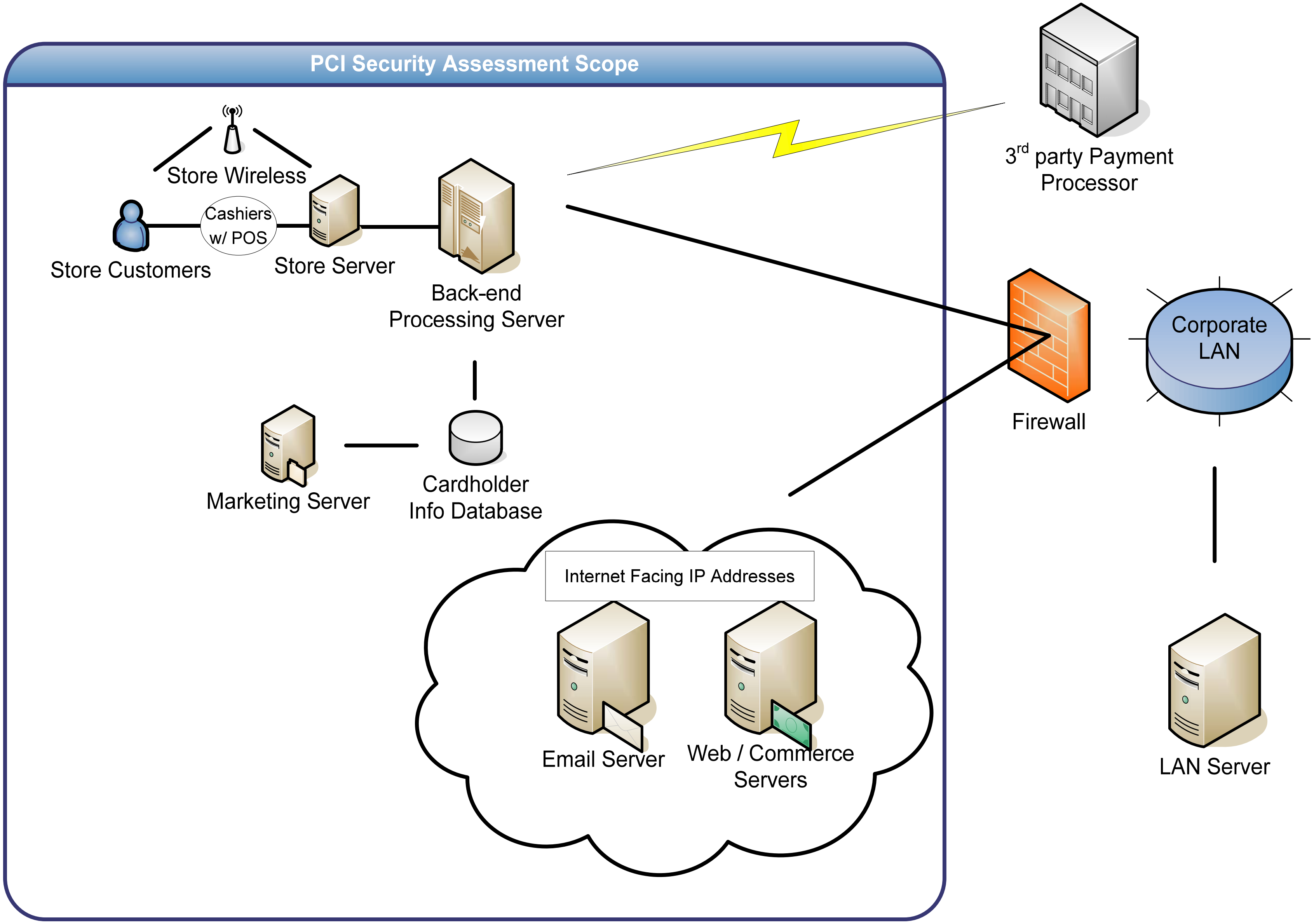


Scope of compliance assessment

Merchants and service providers are also required to conduct a network based PCI security scan.

- Per PCI requirement 11.2, “Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry” (i.e., a 3rd party PCI Approved Scanning Vendor [ASV]).
- The scope of the scan includes all Internet-facing IP addresses; however, the scope can be reduced by:
  - Providing physical segmentation between the network segment handling cardholder data and other segments.
  - Employing appropriate logical segmentation where traffic is prohibited between the segment or network handling cardholder data and other networks or segments.
- If an account data compromise occurs via an IP address or component not included in the scan, the merchant or service provider will be held responsible.

Merchant example



The “30-sec” self-starter

1. Do you store credit card information?

- Do you store track data (information stored on the magnetic stripe on the back of every credit card)?
- If so, is this a requirement of the acquirer?
- If so, do you encrypt the full credit card number (Personal Account Number - PAN)?
- If so, do you mask the PAN when displayed?

2. Are you fully aware of all instances of credit card information in your environment?

- Has your POS systems vendor provided you sufficient assurance that credit card information, including track data, is not stored anywhere on the POS?
- How is credit card information handled in a “store & forward” situation?

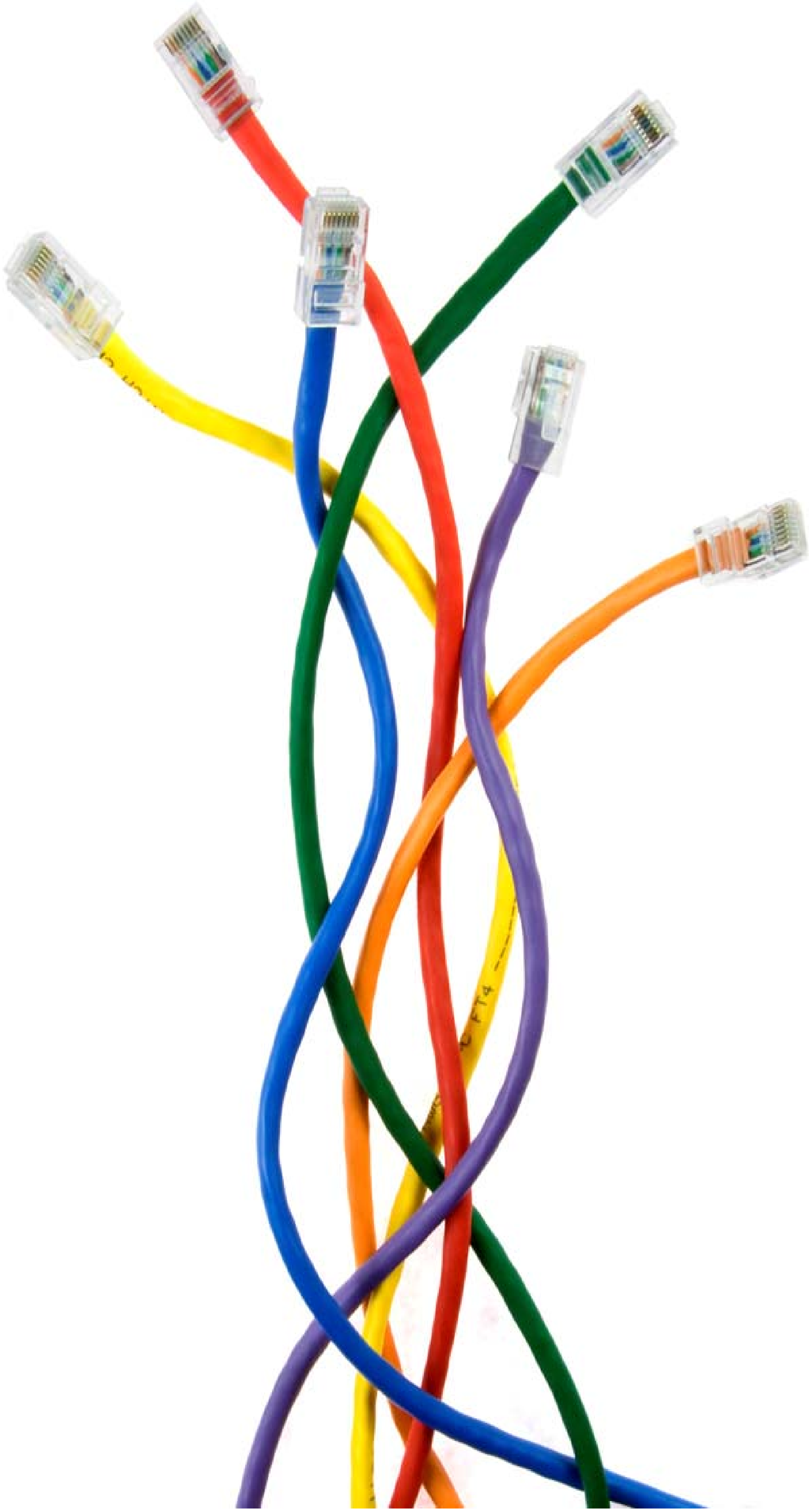
3. Are your POS systems and databases segmented from the rest of your network?

- Do vendors have unrestricted or unmonitored access to the POS environment?
- Do they have any “backdoors” in the POS systems and databases?
- Are you wireless access points and networks secured and segmented from the POS systems and database?
- Are all networks and system regularly patched and reviewed for vulnerabilities?

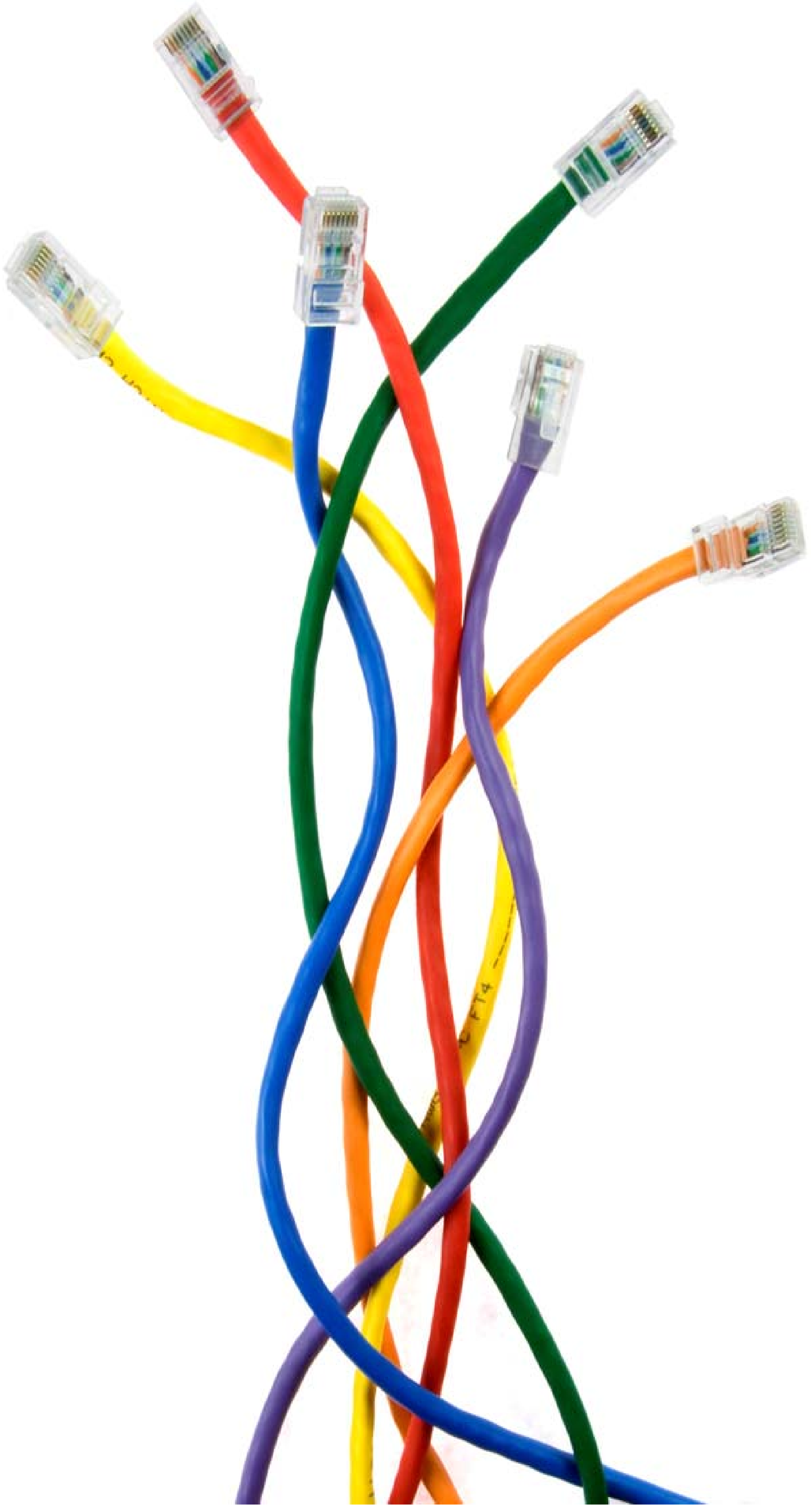
The “30-sec” self-starter

4. **Do you have a well defined software/system development life cycle that incorporates security at all stages?**
    - Do you regularly test your eCommerce web applications for vulnerabilities?
5. **Is credit card information stored only as long as it serves a business purpose?**
    - Do you have a data retention policy?
    - How do you dispose of credit card data?
6. **Is any part of your POS process or IT function outsourced?**
    - Are critical POS systems, databases, reporting or web servers hosted externally?

Roundtable discussion: what are your current challenges?



Common technical challenges and remediation approaches



Common issues

Point of Sale

- Cardholder data in transaction logs and memory (in particular magnetic strip data).
- Lack of encryption during store-fwd mode.
- Legacy equipment: non-unique accounts; inadequate activity monitoring.
- Physical security (POS terminal, PIN PAD, receipts, room keys).

Wireless

- Encryption strength.
- Continual surveillance/rogue device detection/regular scans.
- Vulnerabilities introduced through inadequate wireless architectures.

Web applications

- SQL injection/cross-site scripting/authentication by-pass.
- Poor coding practices/lack of security built into SDLC.

Data leakage/Data integrity

- Lack of role-based access control.
- Lack of adequate audit logging.
- Dealing with data at rest (database encryption, data retention).

Social engineering

- Internal breaches.
- Phishing/pharming.

Scope reduction

An organization can potentially significantly reduce the scope of assessment and remediation efforts by reducing the size of its PCI compliance footprint (i.e., presence of cardholder data within the organization's environment). Potential methods of scope reduction include:

- **Remove data:** Evaluate and remove data where not required, or where duplicate copies exist. Where possible, mask all data when the full credit card number is not required (e.g. reporting applications, etc.).
- **Segment the network:** Isolate systems containing cardholder data within a dedicated network segment to reduce the size of the "cardholder data environment".
- **Consolidate infrastructure:** Where possible, consolidate data stores, systems and system components that contain cardholder data (segregate data views).
- **Modify business processes:** Determine whether business processes can be altered (e.g. order collection, reporting, etc.) to eliminate or reduce the volume of cardholder data or need for specific data elements.
- **Outsource:** Outsource credit card infrastructure components to PCI compliant service providers. For example, consider outsourcing:
  - "Shopping cart" functionality for e-Commerce transactions.
  - Authorization and settlement processing.
  - Internal phone-based order collection systems.

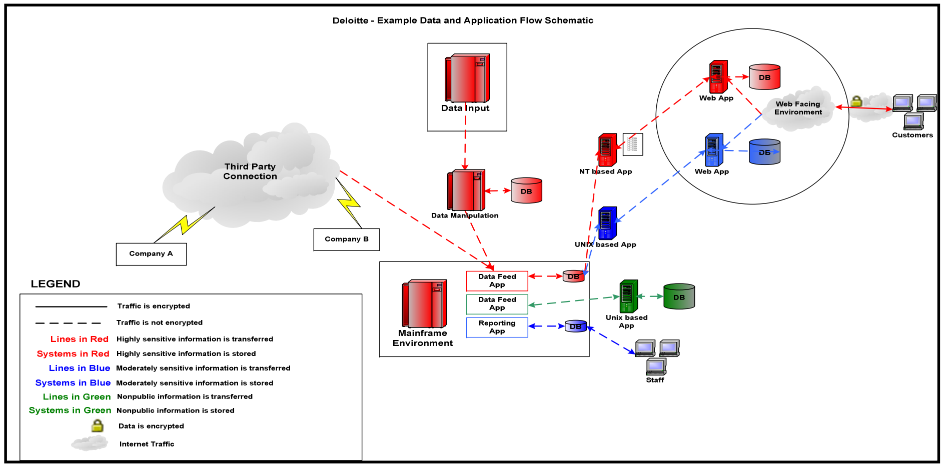
The sustainable approach

Step 1: Identify, review and assess all of your security requirements (including the PCI of course). Rationalize your requirements into a single enterprise security “framework” and manage as part of your overall security program.

Step 2: Embed your security framework (requirements) into relevant business processes.

Step 3: Conduct a data flow analysis and system “inventory” effort to understand the complete lifecycle of the (cardholder) data you wish to protect including:

- Acquisition
- Processing
- Storage
- Usage
- Destruction


Deloitte - Example Data and Application Flow Schematic
Data Input
Data Manipulation
DB
Third Party Connection
Company A
Company B
Mainframe Environment
Data Feed App
Data Feed App
Reporting App
DB
DB
NT based App
UNIX based App
Unix based App
DB
Staff
Web App
DB
Web App
DB
Web Facing Environment
Customers
LEGEND
Traffic is encrypted
Traffic is not encrypted
Lines in Red Highly sensitive information is transferred
Systems in Red Highly sensitive information is stored
Lines in Blue Moderately sensitive information is transferred
Systems in Blue Moderately sensitive information is stored
Lines in Green Nonpublic information is transferred
Systems in Green Nonpublic information is stored
Data is encrypted
Internet Traffic

The sustainable approach

Step 4: Conduct a security risk assessment. Prioritize (risk rank) systems, applications and infrastructure components.

Step 5: Systematically assess the critical systems, applications and components in your environment using your security framework.   Identify gaps, develop solutions appropriate to the risk and remediate.

Step 6: Rinse. Repeat.

Compensating controls

- The PCI DSS allows for compensating controls “…when an entity cannot meet a technical specification of a requirement, but has significantly mitigated the associated risk”.
- Compensating controls must:
  1. Meet the intent and rigor of the original stated PCI DSS requirement;
  2. Repel a compromise attempt with similar force;
  3. Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
  4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.
- Compensating controls may be considered for all requirements EXCEPT storage of prohibited data (i.e. full track data, CVV2, PIN) post-authorization (Requirement 3.2).

Common compliance issues – examples

- Unprotected wireless connections (2.1.1).
  - Where WPA cannot be used, access points should be segregated and virtual private network (VPN) technology used to provide compensating controls. Cardholder data should never be sent over wireless LANs "in the clear" (not encrypted).
- Inability to patch appliances and applications.
  - Where not possible, consider implementing host-based intrusion prevention system (HIPS) to protect against malware.
  - Where HIPS cannot be installed, isolate unpatchable devices behind network based Intrusion Detection/Prevention Systems (IDS/IPS).
  - Segment from the rest of the network and tightly control access.

Other items to consider

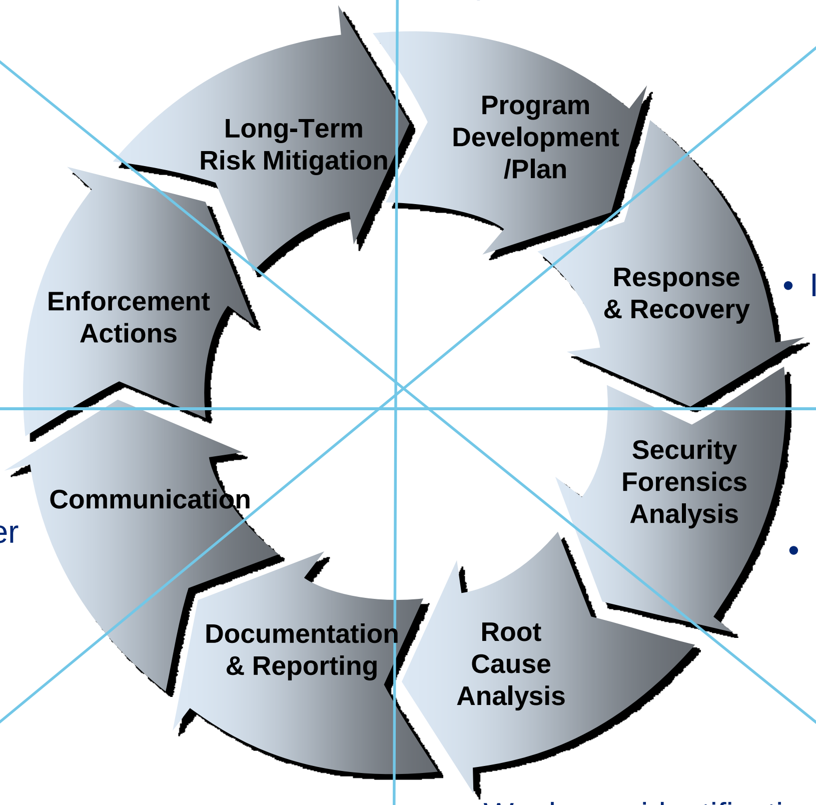
Other items an organization should consider when defining remediation strategies include:

- Develop an **actionable, prioritized roadmap** to facilitate remediation and demonstrate to acquirers and payment brands that compliance issues are being addressed in a timely manner.
- Validate that all 3rd party offerings comply with PCI standards and guidelines. If not, consider replacing or upgrading to verify that:
  - Service providers have undergone a compliance assessment, submitted a Report on Compliance (ROC) if necessary and are identified on the various payment brands' lists of compliant service providers.
  - Payment applications and POS systems comply with the Payment Applications Data Security Standard (PA-DSS).
  - PIN PAD devices do not store PIN or PIN block data and comply with the PCI Pin Entry Device (PED) requirements.
- Inclusion of affiliates or subsidiaries (i.e. the extended enterprise) in assessment and remediation efforts.
- Addressing PCI as a broader initiative (where appropriate).

Be prepared – incident response

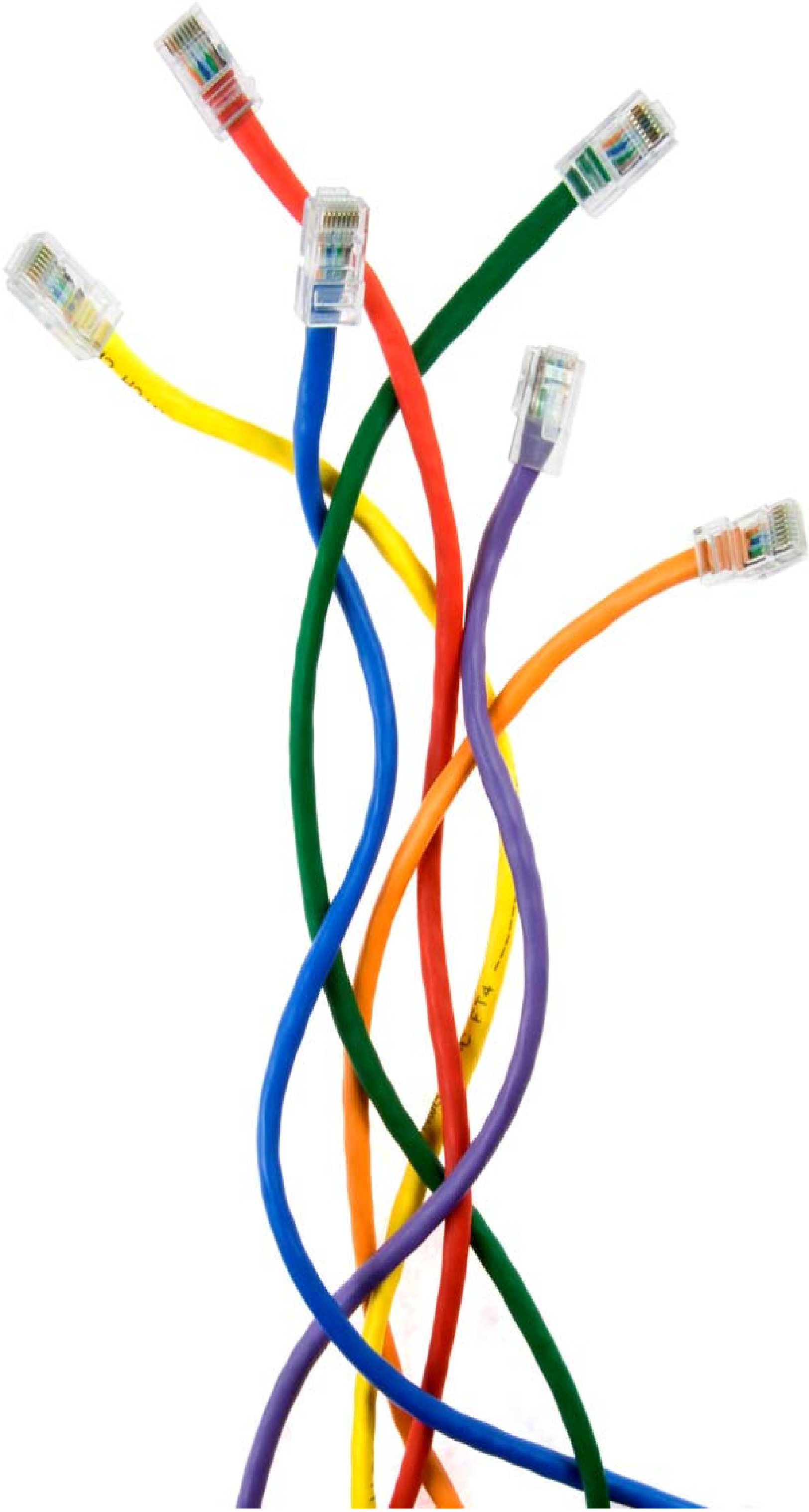
An effective incident response program is critical in helping merchants limit the impact and potential fraud associated with a compromise incident and also prevent future occurrences. Key components of an incident response program include:

- Integration with overall risk management strategy
- Incident response team & procedures

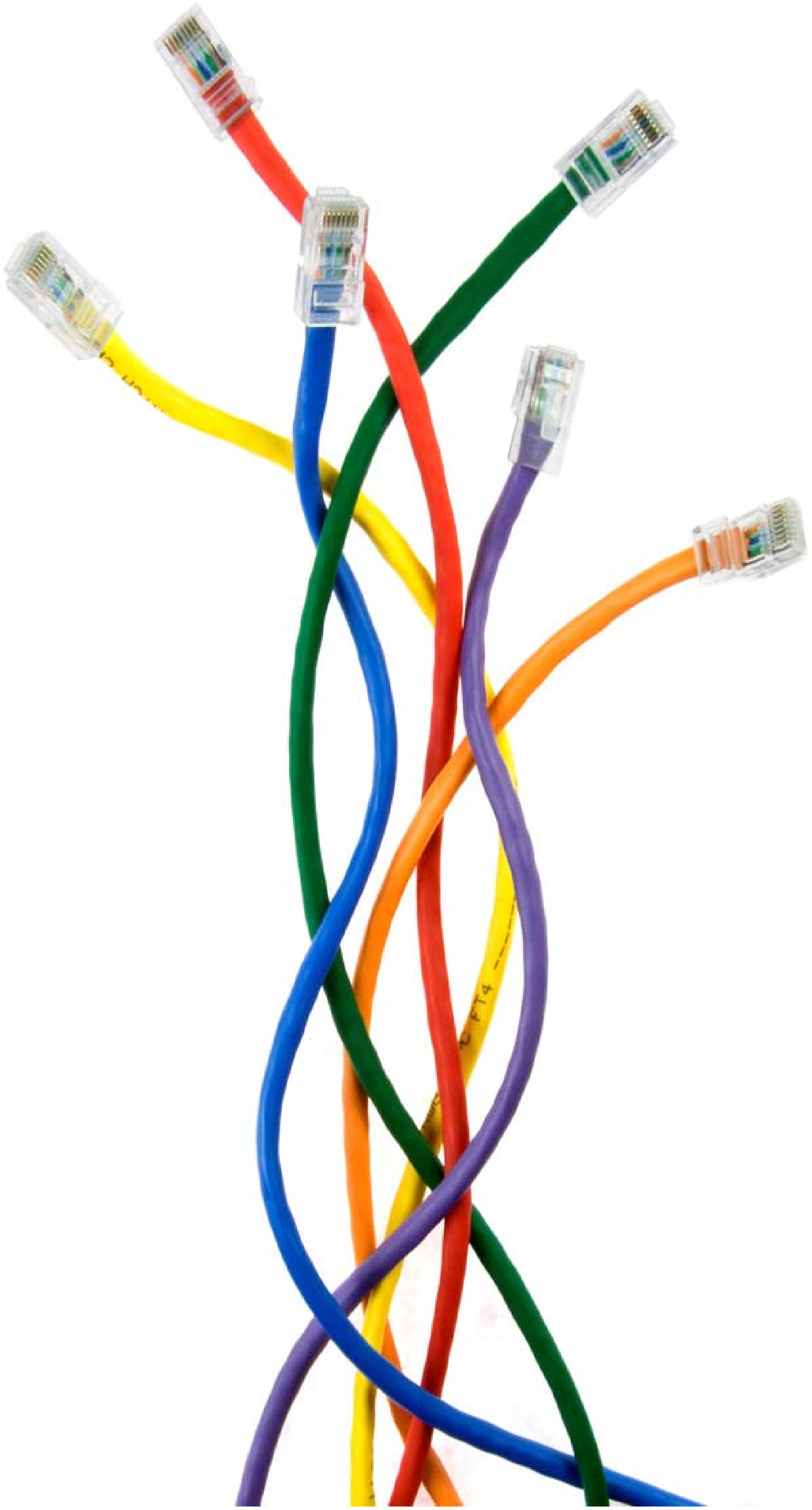

Long-Term Risk Mitigation
Program Development /Plan
Response & Recovery
Security Forensics Analysis
Root Cause Analysis
Documentation & Reporting
Communication
Enforcement Actions

- Evaluation of enforcement options
- Identification and containment
- Communication and broader response strategy (notice)
- Impact and evidence
- Weakness identification
- Reporting

Workplace Technology Services



Questions



Appendix

Payment Card Industry entity responsibilities

Merchant / Service Provider

Responsible for complying with the PCI Data Security Standard (DSS).

Secure and Protect Cardholder Data

Acquirer / Payment Gateway

Responsible for communicating and educating their client (ie. merchant, service provider). Responsible for reporting their client's compliance status to credit card associations.

PCI Security Standards Council

Responsible for creating and maintaining the Data Security Standard (DSS). Responsible for training and certifying PCI auditors.

Responsible for enforcing and monitoring compliance of of Merchant / Service Provider.

Credit Card Association

What are the components of PCI?

Three components of PCI are:

- ***PCI-DSS***

  Data Security Standards – version 1.2
- ***PCI-PA***

  (formerly known as Payment Application Best Practices – PABP)
- ***PCI-PED***

  Pin Entry Device

What level of compliance is applicable?

*1 TPPs and DSEs must use a certified third party to perform the onsite audit

*2 TPPs and DSEs were previously required to have completed quarterly scans and self-assessments by 30 June 2004

Category	Criteria	Requirements	Compliance Dates
Level 1	Merchants >6 MM annual transactions (all channels) All TPPs All DSEs storing data for Level 1,2,3 All compromised merchants, TPPs and DSEs	Annual onsite audit *1 Quarterly network scans	30 June 2005 *2
Level 2	All merchants >1 million transactions annually, but less than 6 MM All merchants meeting the Level 2 criteria of a competing payment brand	Annual self-assessment Quarterly network scans	31 December 2005

What level of compliance is applicable?

Category	Criteria	Requirements	Compliance Dates
Level 3	All merchants with annual ecommerce transaction of >20,000 but less than 1 MM All merchants meeting Level 3 criteria of a competing brand	Annual self-assessment Quarterly network scans	30 June 2005
Level 4	All other merchants	Annual self-assessment Quarterly network scans	Consult acquirer

New Visa Global alignment of deadline

Does not supercede regional deadlines

Category	Criteria	Requirements	Compliance Dates
Level 1	Merchants >6 MM annual transactions (all channels) All TPPs All DSEs storing data for Level 1,2,3 All compromised merchants, TPPs and DSEs	Must not store track 2 data Be fully compliant	October 2009 October 2010
Level 2	All Merchants >1 million transactions annually, but less than 6 MM All merchants meeting the Level 2 criteria of a competing payment brand	Must not store track 2 data Be fully compliant	October 2009 October 2010

Self-assessment questionnaire

SAQ Validation Type	Audience	SAQ	Description
1	Merchants	A (11 questions)	Card not present (e-commerce or mail/telephone order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.
2	Merchants	B (21 questions)	Imprint-only merchants with no electronic cardholder data storage.
3	Merchants	B (21 questions)	Stand-alone terminal merchants, no electronic cardholder data storage.
4	Merchants	C (38 questions)	Merchants with POS systems connected to the Internet, no electronic cardholder data storage.
5	Merchants and all service providers	D (226 questions)	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.

Deloitte.