



PCI compliance –
business track
Executing through
excellence



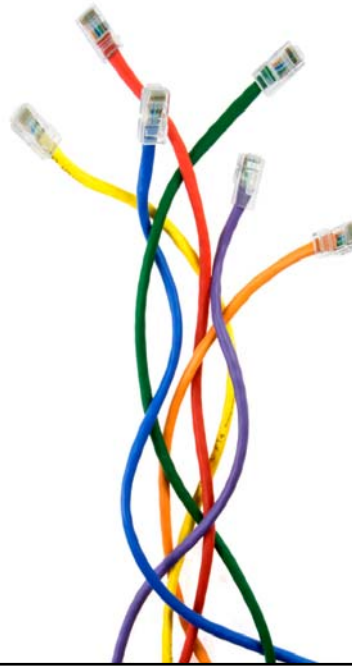
Tejinder Basi, Partner
Nazam Jamal, Senior Manager
May 27, 2009

© Deloitte & Touche LLP and affiliated entities

Agenda

1. Introduction
2. What are the challenges that organizations face?
3. How do we get a “return on investment”?
4. Compliance tools
5. What lessons have we learned?
6. Open discussion – questions

What are the challenges that organizations face?



2 PCI - Executing through excellence

What challenges do you face?

- Notes on flip chart

3 PCI - Executing through excellence

© Deloitte & Touche LLP and affiliated entities

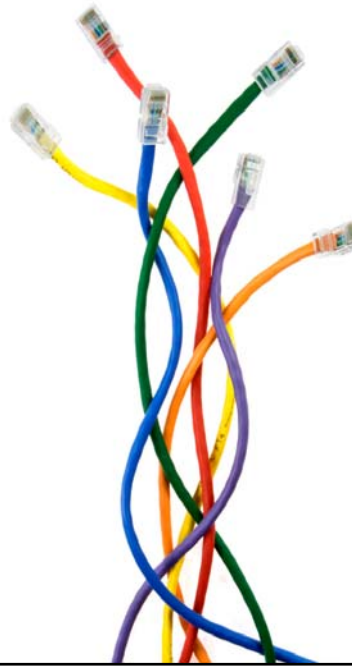
The current reality & challenges – environmental

- Continued lack of understanding as to who the standard applies to, compliance deadlines and penalties.
- Communication about compliance (deadlines, ramifications etc.) is not effective or in some instances non-existent.
- PCI is NOT part of broad regulatory/audit/compliance and therefore there is no ongoing oversight or program/strategy in place to sustain compliance.
- Lack of effective controls over the “Point of Sale” terminals, allowing the possibility of tampering & compromise of confidential data.
- Lack of strategy in dealing with “card not present” fraud.

The current reality & challenges – organizational

- Organizational silos prevent a holistic view to the magnitude of the problem and create subsequent losses.
- Fraud is seen by many organizations as a “cost of doing business”.
- Approach to compliance does require the involvement of multiple stakeholders
- There is no clear enterprise-wide owner/sponsor.
- The traditional way of compliance (letter of the law) proves to be very costly or impractical.
- Building a business case to justify to the business the need for compliance & ROI.
- Widespread access to critical data – “grandfather rights”.
- Lack of effective access controls.

How do we get a
return on
investment?



6 PCI - Executing through excellence

Common sense approach to achieving compliance and getting a “return on investment”

- Deloitte’s approach takes into account the original problem (fraud, data loss, data breaches, brand impact) that the PCI standard was developed to address, thereby taking a broader perspective so that organizations can get a return on their investment.
- A carefully thought through, holistic and risk-based approach is required to take advantage of the synergies that exist between PCI compliance & other compliance requirements (e.g. SOX, AML etc).
- PCI compliance includes PCI-DSS, PCI-PED, PCI-PA, Chip & Pin implementation (POS).
- “Recurring” and “card not present” payments and the changes to the chargeback process should be taken into account.
- Examine other approaches as alternative i.e. tokenization, as it can significantly reduce PCI scope.
- The best approach is to “do it once and satisfy many”.
- This approach will help reduce the overall effort, optimize operations and produce a return on investment.

7 PCI - Executing through excellence

© Deloitte & Touche LLP and affiliated entities

How to approach PCI as part of a bigger solution

- Understand fraud losses, data losses & breaches, security and data protection challenges faced by your organization – all the pain points.
- Build a value proposition beyond just compliance.
- Many of the processes have been derived from the paper-based business and do not necessarily reflect the current environment or need.
- Merchants must be compliant to accept chip & PIN at their Point of Sale by October 2010, or face a liability shift (i.e. they absorb the loss).
- Review of other similar synergies are at play and can be leveraged.

Data: asset & liability

Data is both an asset and a liability. As organizations grow, the volume and complexity of data increase to support the business. Certain types of data within the enterprise must be protected against theft, loss, and misuse.

This data includes:

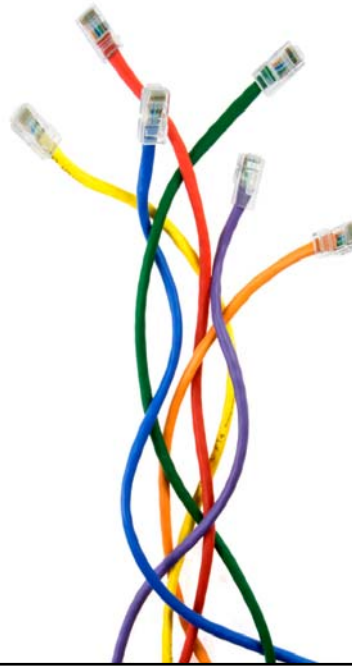
-  **Credit card data**
-  **Patent or trade secrets**
-  **Customers' information**
-  **Corporate information**
-  **Personally identifiable information**

Without an effective method to:

- **Discover** data, it is difficult to apply the appropriate security controls to it
- **Classify** data, it is difficult to understand the importance and sensitivity of the data
- **Control** data, it is difficult to restrict access to data, prevent misuse of it, and secure it at rest and in transit
- **Audit** data and its usage, it is difficult to enforce the security controls

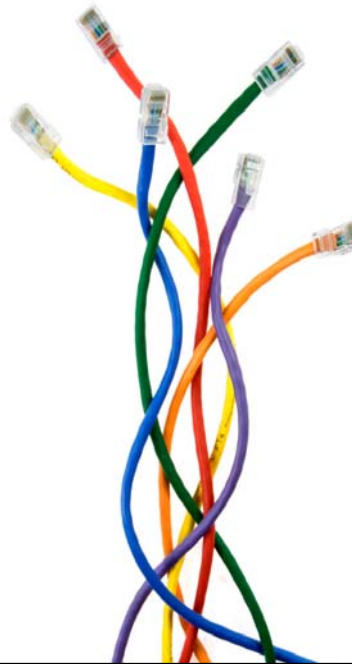
As a result, it is difficult to adequately **protect** data throughout its life cycle across the enterprise

Compliance tools



10 PCI - Executing through excellence

What lessons have we learned?



11 PCI - Executing through excellence

Observations & lessons learned

- Communication & awareness has been lacking, minimizing the chances of effective & timely implementation and benefits to the organization.
- All stakeholders have not been involved with PCI.
- Many organizations are doing the minimum just to comply, thereby putting their brand at risk.
- Organizations are storing data that is not required to conduct the business successfully, leading into redundant processes & storage of redundant and unnecessary data.
- Some organizations are repeating the exercise as their challenges were not dealt with properly in the first instance .
- The approach to PCI compliance process, by some organizations, is a one time effort, and thus NOT sustainable.
- Duplication/repetition of work instead of “do it once and satisfy many”.

Observations & lessons learned

- PCI has not been part of the overall security framework and is seen as a “credit card” problem only.
- Process for the development of new applications/processes in some instances does not take into account the PCI standards requirements to keep the organization compliant.
- Some credit card processing has been outsourced without due diligence to whether the outsourced organization is in fact PCI compliant. Outsourcers do in fact outsource some of the work further down the stream compounding the problem.
- Some organizations have embarked upon remediation, without first doing data classification/discovery, to ensure that they limit their encryption and protection strategy to sensitive data.
- The road to PCI compliance does cross many departments and therefore must have buy-in from the top; otherwise organizations risk failure and/or continued exposure.

Observations & lessons learned

- Contracts managing third parties do not keep pace with changing business needs and in some instances, have not stipulated the right to audit the third parties. Statement printing, frequent flyer programs, loyalty programs, target marketing have been outsourced by many organizations without adequate oversight ability.
- We have encountered situations where scanning of applications and networks have been generic and not deep enough thereby providing a false sense of security.
- There does not appear to be an effort to utilize “compensating controls”. This has significant impact where legacy systems are involved or where organizations may have invested in a different approach/technology to secure themselves.
- Attestation is a challenge due to inconsistency of interpretation or experience of QSA, especially where it involves compensating controls.
- PCI and chip & PIN projects are dealt with differently. They both carry liability shift and impact the same area of the business with synergy. Furthermore, combining the two can reduce the scope of PCI.

Example

Existing document vaults need to be compliant

- Document storage is not compliant with PCI-DSS as organizations are not encrypting the data, nor are they aware of the PCI requirement to encrypt documents. These include:
 - Transactional documents, statements, invoices.

Retrieval of documents

- Ability to send and deliver secure and encrypted documents. Customer Service Rep’s pull up invoices from storage as needed. User access control allow people to see only what they need to see.

Document production

- From creation of the bill/statement to production must be secure.

Data quality

- Ensure bills and statements are being sent to the right address and name.

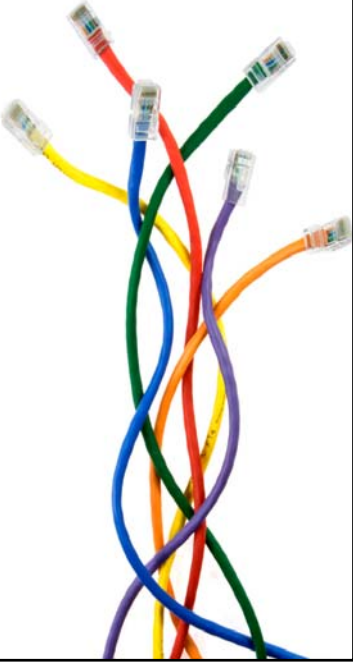
Achieving compliance does not necessarily mean becoming secure. However, achieving security does translate into compliance.

PCI is not just an IT issue

PCI is a business issue

PCI is a journey

Open discussion –
questions?



18 PCI - Executing through excellence

Appendix A

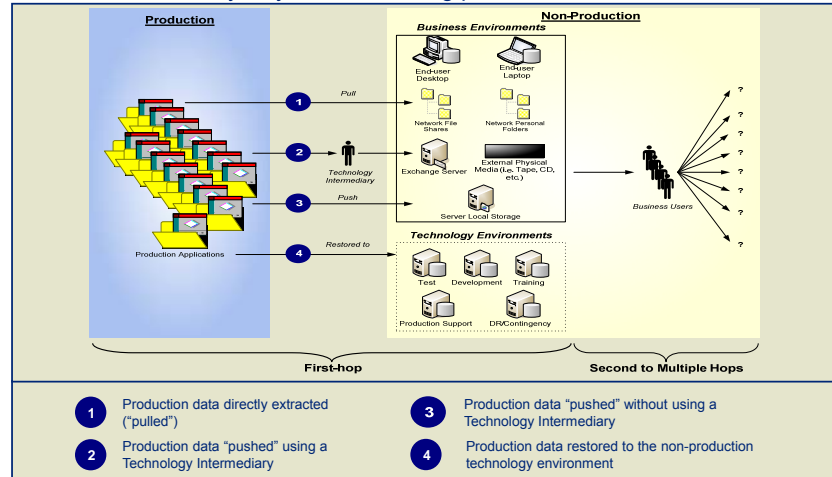
Case study – Data leakage

19 PCI - Executing through excellence

© Deloitte & Touche LLP and affiliated entities

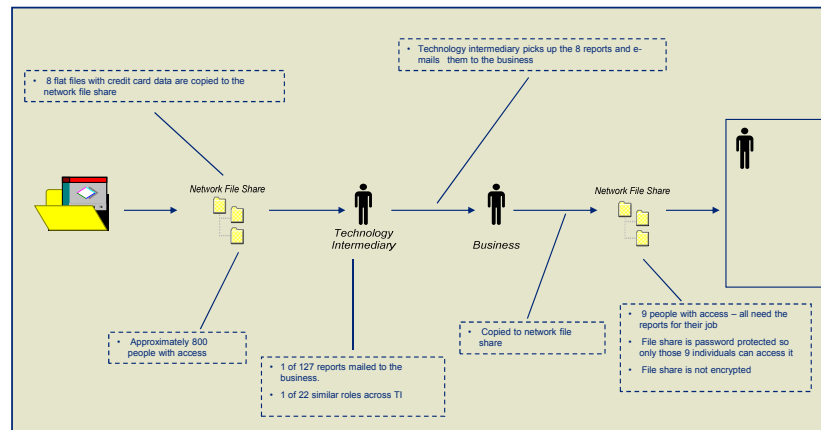
How data leaves production (data discovery)

Data is leaving the production environments through various channels. Outlined below are the four key ways data is leaving production.

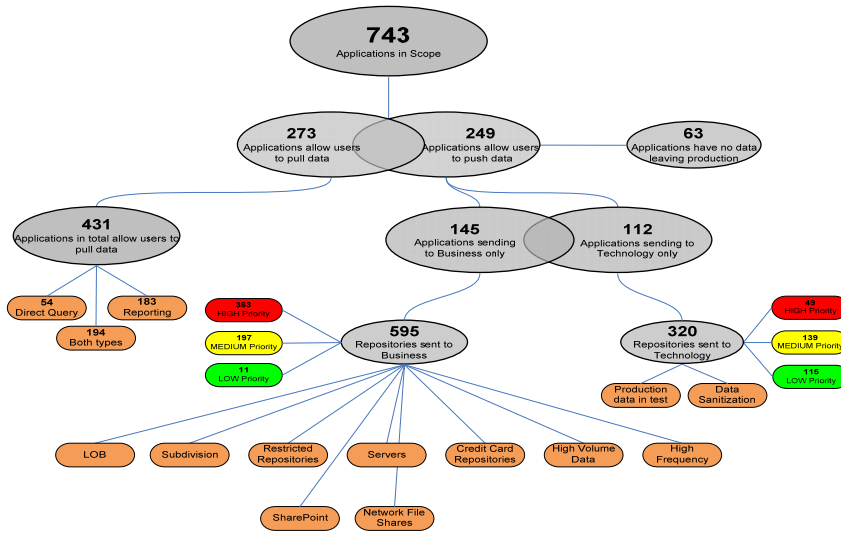


Data flow scenario

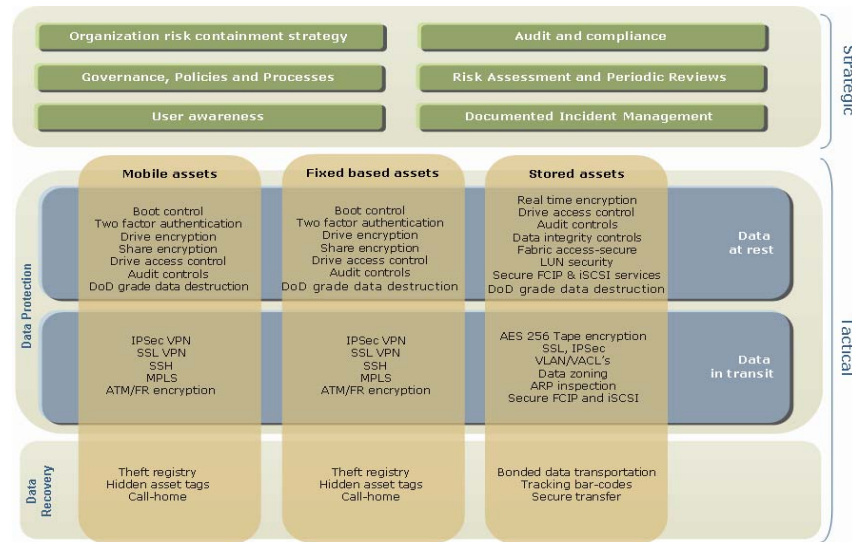
The following example outlines the flow of eight reports with credit card data moving from production to a global share and finally to a network file share for use by the business.



Understanding the magnitude of data leaving production – (risk assessment)



Data protection summary



Deloitte.