




PCI @ Bell Canada

Luc Jarry, CGEIT

Bell Canada – Corporate Security

Welcome

- *The purpose of this presentation is to share with you some experience about PCI compliancy.*
 - *The scope of this project is for Bell to achieve PCI compliancy as a merchant.*
 - *Some of these approaches may or may not apply to your enterprise depending on the size, the merchant level and the scope of your PCI effort.*
 - *If you have any questions / comments, please ask!*
- 



Agenda

- **Welcome**
- **Bell Canada as a merchant**
- **PCI work streams**
- **PCI work flow**

Bell Canada as a merchant

- Bell processes 23M credit card transactions per year for ~ \$1.4B
- Three entry points of credit cards information:
 - On line services (www.bell.ca)
 - Call centers (310-bell)
 - Bell stores
- Services Impacted:

Wire lines

Bell TV

Wireless

Bell Internet

Each entry points are considered as Level 1 merchant

Bell Canada as a merchant (Con't)

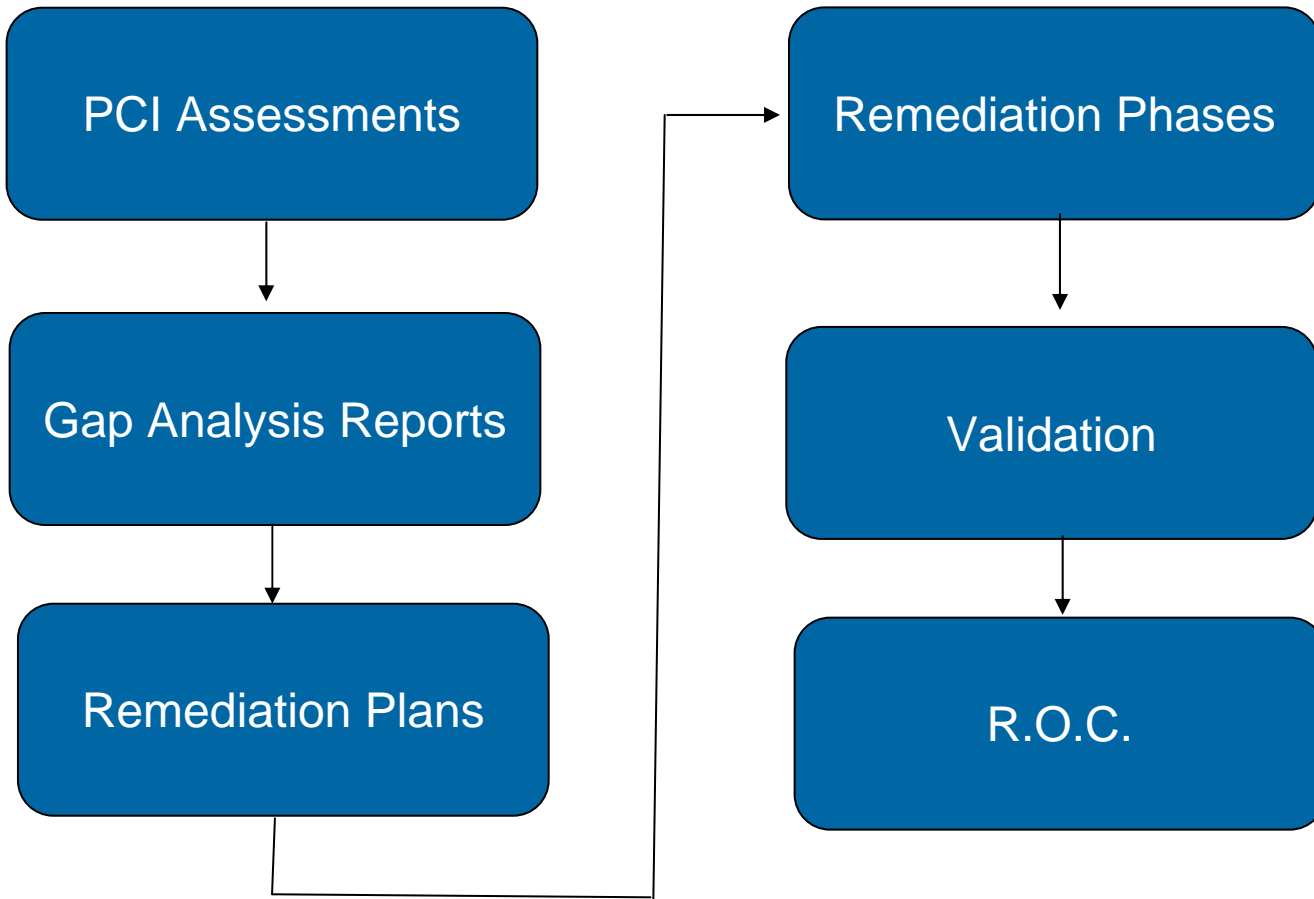
- Bell Canada's network is across Canada
- Many services providers involved: CGI, IBM, etc.
- Billing is outsourced to Amdocs
- Bell has business reasons to retain cardholder data for billing reoccurrences and customer purchasing profiles.
- Retail: Bell has over 500 point of sales (POS) across Canada including Bell World stores, kiosks and dealers (Sources, Sears, Circuits, etc)

PCI scope varies on the business needs of keeping cardholder data

PCI work streams at Bell Canada

1. **Vulnerability scans on external channels:** Over 650 internet facing IPs were scanned on 11 different DMZs.
2. **Common Infrastructure:** This would be all infrastructure that supports the applications with cardholder data: network (ICN), network management, firewalls, security policies & standards, virus protection, etc, etc.
3. **Modernized applications:** That store, process and transmit cardholder data in a modernized (recently developed) application.
4. **Legacy applications:** That store, process and transmit cardholder data in a application running on legacy operating environment such as mainframe (OS 390 & RACF), apps written in JCL with DB2, etc.
5. **Amdocs:** Is the main service provider that performs millions of credit card transactions in the name of Bell Canada.

PCI Workflow



PCI Workflow (Con't)

1. PCI assessment:

- Consist of assessing the common infrastructure and the applications based on the 231 applicable PCI security controls.
- Although PCI-DSS is prescriptive, doing the assessments happens to be a complex exercise.
- You need resources that have strong PCI knowledge with auditing experience. Preferably QSA.

2. Gap Analysis Reports:

- Are based on the PCI-DSS security controls.
- The purpose is to identify what are the PCI security controls that are **In Place (Passed)** and **Not In Place (Failed)**.
- The gap analysis reports must provide details on all controls: what was observed, with who, when, how, etc.

PCI Workflow (Con't)

3. Remediation Plans:

- Remediation plans will provide in detailed the necessary actions required to address the PCI security controls that were identified as **Not In Place** in the gap analysis reports.
- A remediation plan is required for each gap analysis report.
- Funding requirements must also be addressed.

4. Remediation Phases:

- Are the actual projects that will remediate the necessary PCI requirements.
- Experienced project managers with PCI-DSS knowledge is a must.
- Centralized governance is strongly recommended.

PCI Workflow (Con't)

4. Validation:

- Is the actual PCI audit normally performed by a QSA.
- At that phase, the Not In Place must be validated

5. R.O.C.:

- Report On Compliance
- Many ROC may be required

About the PCI assessments

- **Preparation is key:**
 - ✓ Prepare a document that explains in a business language what PCI is, the purpose of the assessment, etc.
 - ✓ Send in advance the PCI security controls that are applicable.
 - ✓ Let the business owners know in advance the resources that will be required for the assessments (Sys Admin, DBA, Developers, Sys support, etc).
 - ✓ Let the business owner know that a flowchart will be required to understand how cardholder data flows in the system (in & out). Usually such chart does not exist.

About the PCI assessments (Con't)

- **During the assessment:**
 - ✓ You must first determine with the business owner the business needs of storing cardholder data to see if the application can be put “Out of Scope” of the PCI audit. Business justifications are:
 - Monthly Reoccurrences
 - Customer profiles for online shopping
 - Fraud detection
 - ✓ Start the assessment by looking at the data flowchart of the cardholder data. You need to understand how cardholder data is received, how it is processed, where and how it is stored and where and how it is sent. If needed use a white board.

PCI-DSS has 128 testing procedures that apply to applications

About Remediations

- **The remediation work streams:**
 - **Internet Facing IPs:** Addressing vulnerability scans with severity 3 & higher. Building tools for future remediations and remediation efforts are being done by service providers.
 - **Common Infrastructure:** Creation of CDE with network segmentation and DMZ with PCI security controls. Many remediation plans addressing documentations such as security policies, standards and CC diagrams. Remediation efforts on physical security of data centers, etc, etc.
 - **Applications:** Both modernized and legacy

Some Experiences (in no specific order)

- Usage of technology to reduce PCI scope
 - **Format Preserving Encryption (FPE):** Data encryption while preserving the same data format. FPE is not an approved mode of AES algorithm and it is not FIPS compliant. Bell did not select this technology because encrypted PAN is still considered as PAN.
 - **Tokenization:** Tokenization replaces cardholder data with a token. The token is very similar of a credit card number. Every time a credit card number is captured, a unique token is assigned. The cardholder data is kept on a safe server. Bell is testing this technology because a token is not considered as PAN.
- Network Segregation: Creation of a Cardholder Data Environment (CDE). The goal is to segregate all payment cards applications and concentrate the PCI audit in one network segmentation.

Some Challenges (in no specific order)

- Understanding of PCI in general (executives, business owners, users, etc)
 - PCI is considered as an “Extra Cost of Doing Business”.
 - Senior executive’s reaction: *How can we get out of it ?*
 - PCI awareness in general (Marketing groups, Business offices, Call centers, etc)
 - Understanding of what is; “In and Out of Scope” of PCI
- PCI Scope: Inventory of applications that store, process and transmit cardholder data.
- Funding \$\$
- Section 12.8 (For outsourced services)

Bell

Questions ? : [Luc Jarry \(luc.jarry@bell.ca\)](mailto:luc.jarry@bell.ca)