PCI Implementation: Lessons Learned from a Transit Perspective

Paul Korczak, Project Manager

New York City Transit
Lessons Learned:

- Obtain support of top management sponsor(s) early on.
  - Management needed to understand the full import of the project.
    - Business implications.
    - Benefits.
    - Costs.
  - Management needed to support a “top down” approach” to get the job done timely.
  - Management support facilitated communications and interactions among stakeholders and assured dedication of sufficient resources.
Lessons Learned:

- Assemble the appropriate internal team.
  - Business.
  - Technical.
  - Financial.
  - Your fare collection system vendor.

- Establish a formal process and timeline at the start; use your QSA for guidance.
Lessons Learned:

➢ Build employee awareness and encourage open dialogue.
  ➢ Employee comments and suggestions have been a critical part of the compliance process.
  ➢ Facilitated changes to day-to-day business processes and procedures.
Lessons Learned:

- Make a first attempt to scope out the vulnerabilities early on.
  - Expedite efforts with stakeholders (including your system vendor) to identify and eliminate prohibited sensitive-data stored within the cardholder environment.
  - Look closely and everywhere.
  - Be realistic about timelines; for transit, some requirements may be new and difficult to achieve.
  - Identify areas where remediation efforts can move ahead concurrently.
Lessons Learned:

- Begin discussions with QSA regarding details of technical positions/environment early on, even during selection process.
  - Procured Qualified Security Assessor (QSA) to provide on-site compliance validation and vulnerability assessment services to systems and processes managed by NYCT.
  - Pre-selection discussions with QSA technical staff may have resulted in more accurate setting of expectations.
Lessons Learned:

- Work closely with QSA, card processor, card brands (if possible) and/or internal staff to align expectations and strategy.
  - In conjunction with QSA, developed compliance gap analysis and addressed open items in a systematic approach to achieve compliance as quickly as feasible.
  - Regular communications among each of the affected internal departments allowed NYCT to address items immediately or identify achievable timelines for completion.
  - Improved communications with card processor and card brands may have facilitated overall alignment of compliance effort across applicable organizations.
Lessons Learned:

- Rethink ways of doing business – review every use of cardholder data to see if it is really needed
  - Examined our business, analyzed where cardholder data is being stored, and investigated & questioned the underlying business needs for such information.
  - We determined that we could change our business processes and systems to eliminate any retention of cardholder in some cases.
  - All options on the table: business process changes, technical and system changes, etc.
  - Undertook a significant effort to completely eliminate the electronic storage of any credit card numbers by NYCT on systems used for 2 account based customer programs.
Lessons Learned:

- Adjust on-going initiatives as needed to meet requirements and identify potential procurement issues early
  - NYCT had ongoing internal projects that, while pre-dating PCI compliance efforts, would address various PCI requirements. Implemented shorter-term interim solutions that are compliant while expediting the larger projects as a whole.
  - For agencies with strict formal procurement procedures, tight deadlines imposed by outside entities for compliance may contrast with normal procurement processes and timelines.
Lessons Learned:

➤ Don’t give up! It’s worth the effort!