PCI DSS
CASE STUDY

By
J. FLUKER

Table of Contents

Case Study: Assisting Transport for London (TfL)

Date: March 8th, 2023

Name of Company Hired: NCC Group

Case Type: PCI DSS (Payment Card Industry Data Security Standard)

At a Glance

Organization: Transport for London

Industry: Transportation

Challenge: To provide TfL with the cyber assurance and PCI DSS compliance necessary to roll out its contactless payment project across various methods of public transportation.

Solution: NCC Group worked with TfL and their supplier to develop a suitable framework that would satisfy the requirements and provide a point-to-point encryption (P2PE) standard.

Result: NCC Group's services helped assess potential security vulnerabilities and provided peace of mind for TfL's contactless payment project.

Situation

NCC Group was appointed by Transport for London (TfL) to ensure that all elements of its contactless payment technology system operated within the scope of the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents. As an Approved Scanning Vendor (ASV) and with a team of Qualified Security Assessors (QSAs).

NCC Group has a wealth of experience in helping organizations achieve PCI compliance. Its “one-stop shop” set of PCI DSS compliance services, including QSA advisory, audit, ASV scanning, and penetration testing, is specifically aimed at assisting organizations to quickly achieve and then crucially maintain compliance.

Challenge

At that time, there wasn't a point-to-point encryption (P2PE) standard, so NCC Group worked with TfL and their supplier to develop a suitable framework that would satisfy the requirements of the card schemes and would provide a meaningful standard against which compliance could be measured.

The compliance framework eventually became the Pin Transaction Security (PTS) v 3.1 standards for the device itself, Point to Point Encryption standard v 1.1 for the transmission of data from the device to the data center, and PCI DSS standard v 2.0 for the data center itself. Using this compliance framework, NCC Group then undertook a series of "gap analysis" exercises on the data center, the P2PE solution, and the various environments in which the devices would operate and be stored.

Solution

During the remediation program that followed, NCC Group provided a considerable amount of advice and guidance on how to implement the various aspects of the solution. Once through the remediation program, NCC Group undertook a PCI DSS assessment and P2PE assessment on the overall solution, as well as undertaking a penetration test on the device itself. The outcomes of the assessments were presented to the card schemes and were subsequently given a green light for the project.

Result

TfL initially launched the contactless payment scheme on buses and is in the process of rolling it out to passengers traveling via the Tube, tram, London Overground, DLR, and most National Rail services in London. The bus launch went live in December 2012, and TfL was commended for its approach to security, with its credit card acquirer describing it as "exemplary".

NCC Group acted as an independent, trusted advisor and assessed the potential security vulnerabilities of the solution to give us peace of mind that the security was sound."

Following the initial bus launch, NCC Group is continuing to work on the full implementation across the remaining transport methods.

"NCC Group acted as an independent, trusted advisor and assessed the potential security vulnerabilities of the solution to give us peace of mind that the security was sound." -- Phil Jones, Head of Payment Security Barclaycard[1]

Armchair Observations

We know what solutions NCC Group implemented, but let's examine other solutions, why they're important, and the positive impact these solutions would have on Transport for London. Ready, set, go!

Keeping the budget and time frame in mind (March 8th, 2023) here are more solutions that could strengthen the rollout of Transport for London's (TfL) contactless payment system:

Solution No. 1: Continuous Security Monitoring and Threat Detection

Why It Matters

No matter how many risks are mitigated or flat out eliminated, a one-time assessment can't protect against evolving threats.

How It Helps

Real-time threat detection systems (e.g., SIEM, IDS/IPS) monitor payment systems for suspicious activities continuously.

Business Impact

- ✓ **Reduces downtime by detecting and responding to threats early, before they cause widespread disruption.**
- ✓ **Protects customer trust by minimizing the risk of publicized breaches.**
- ✓ **Saves costs by preventing damage from cyber attacks rather than reacting after they occur.**

[1] *Case Study: Assisting Transport for London (TfL)* (March 8th, 2023), https://www.nccgroup.com/us/case-study-pci-dss-for-transport-for-london/

Solution No. 2. Red Team Exercises and Penetration Testing

Why It Matters

Proactively tests the resilience of the system beyond standard vulnerability scans.

How It Helps

Conducts regular red team simulations to mimic sophisticated attacker techniques targeting payment systems and infrastructure.

Business Impact

- ✓ **Identifies weaknesses that standard audits might miss, strengthening system resilience.**
- ✓ **Demonstrates due diligence to regulators and stakeholders.**

  Improves response readiness, reducing the impact of real attacks.

Solution No. 3. Security Awareness Training for Staff and Vendors

Why It Matters

Human error is a major contributor to security breaches.

How It Helps

Trains TfL staff and third-party vendors on secure handling of payment systems, social engineering threats, and PCI DSS responsibilities.

Business Impact

- ✓ **Reduces human error, which is a leading cause of security breaches.**
- ✓ **Boosts operational security culture across internal and external teams.**
- ✓ **Lowers compliance risk by ensuring policies and procedures are understood and followed.**

Solution No. 4. Zero Trust Architecture

Why It Matters

Reduces implicit trust and limits lateral movement if breached.

How It Helps

Implements access controls and network segmentation around payment environments to ensure minimal access and verification of all users and devices.

Business Impact

- ✓ **Limits breach scope, reducing the potential damage of internal or external attacks.**
- ✓ **Improves data protection, particularly important for customer financial data.**
- ✓ **Enhances regulatory compliance, as Zero Trust aligns well with modern security frameworks.**

Solution No. 5. Tokenization in Addition to P2PE

Why It Matters

Tokenization replaces sensitive data with non-sensitive equivalents, further reducing PCI scope.

How It Helps

Introduces tokenization for cardholder data both in transit and at rest, in conjunction with P2PE.

Business Impact

- ✓ **Reduces PCI DSS scope, saving on ongoing compliance costs.**
- ✓ **Improves customer privacy, which can strengthen brand loyalty.**
- ✓ **Minimizes liability in the event of a breach, since actual card data isn't stored.**

Solution No. 6. Third-Party Risk Management Enhancements

Why It Matters

Suppliers can introduce vulnerabilities into the system.

How It Helps

Conducts security assessments of all third-party vendors involved in the payment system lifecycle and enforce strong contractual cybersecurity obligations.

Business Impact

- ✓ **Prevents supply chain compromises, which are increasingly targeted by attackers.**
- ✓ **Protects brand reputation, since customers don't differentiate between internal and third-party breaches.**
- ✓ **Ensures smoother operations, as secure vendors are less likely to suffer downtime.**

Solution No. 7. Automated Compliance Management Tools

Why It Matters

PCI DSS compliance is ongoing and can often be complex.

How It Helps

Uses compliance automation platforms to continuously monitor and report on PCI DSS requirements across the infrastructure.

Business Impact

- ✓ **Reduces manual effort and errors, lowering staff time and overhead costs.**
- ✓ **Ensures continuous compliance, avoiding penalties or fines.**
- ✓ **Improves audit readiness, making it easier to demonstrate compliance at any time.**

Solution No. 8. Multi-Factor Authentication (MFA) Across All Payment Admin Interfaces

Why It Matters

Prevents unauthorized access to sensitive systems.

How It Helps

Requires MFA for any administrative access to systems handling payment processing or customer data.

Business Impact

- ✓ **Prevents unauthorized access, particularly from credential theft.**
- ✓ **Supports regulatory requirements, such as GDPR or PCI DSS.**
- ✓ **Boosts customer confidence, knowing strong protections are in place for their data.**

Summary

These additional solutions would enhance resilience, compliance, and ongoing assurance, making the system better equipped to handle emerging cybersecurity threats and regulatory requirements.

Overall Business Benefits Across All Solutions

- ✓ Enhanced operational continuity
- ✓ Strengthened public confidence and reputation
- ✓ Improved regulatory compliance and audit performance
- ✓ Reduced financial and legal exposure
- ✓ Increased customer adoption of contactless services due to perceived security

Thanks for kicking back with me for a while. Cheers!