2024 Best Practices Submission

Presentation Title:
Defending the Plastic Kingdom: A PCI Adventure

Presenters:
Steph Smith, Senior Managing Director, Cash and Credit Management Services, Texas Tech University

Christine Jones, Assistant Managing Director, Cash and Credit Management Services, Texas Tech University

Presentation Description:
Defining what PCI DSS (Payment Card Industry Data Security Standards) is, who is responsible for it and how Texas Tech University navigated their PCI adventure across the campus.

_____

Statement of the Problem:
Texas Tech realized we needed to better understand our payment card processing environment to ensure both compliance with the Payment Card Industry Data Security Standards and reducing risk of credit card fraud. Technology and security standards are constantly evolving, and Texas Tech knew we needed to streamline our processes to keep systems from being implemented without appropriate security review and also to identify any processing methods that may no longer be compliant with current standards.

Identify the Solution:
Texas Tech contracted with a PCI service vendor so our merchants could talk directly with a Qualified Security Assessor and identify any potential areas of risk. We conducted on-site audits with merchants, implemented a system for more efficient annual compliance attestations and provided updated training to campus merchants. The university policy was updated and provided to merchants to outline merchant responsibilities and requirements for P2PE equipment. Texas Tech contracted with a specific vendors to provide cost effective P2PE equipment, which significantly reduced our PCI scope and ultimately reduced our risk for fraud. This in turn saved the university noncompliance fines, fees for scanning and penetration testing, which was no longer needed, and potential breach costs, which are significant.

Implementation Timeline:

Year 1 – Re-wrote the university policy outlining payment card processes, department responsibilities, equipment requirements and compliance regulations.

Year 1 – Had Qualified Security Assessor (QSA) do an assessment of the Texas Tech payment card environment through a sampling of merchants. Subsequent months after this – Worked to remediate any areas of potential risk that were identified in the QSA assessment and began on-site audits by Texas Tech staff to fully understand remaining payment card environment.

Year 2 – Implemented system which included a Self-Assessment Questionnaire (SAQ) portal to efficiently assign, monitor, review and approve annual SAQs for approximately 200 merchant accounts. The system also included a document locker for effectively collecting required documentation to support compliance that could be easily accessed and reviewed.

Subsequent months – Created training materials for merchant to help them gain a better understanding of the PCI requirements and SAQs. Will be implementing a new training module this year.

Benefits & Retrospect:
Texas Tech is effectively reducing our PCI scope, which results in a reduction in potential risk for credit card fraud. In a world where online fraud and internet scams are ever increasing, we are able to better inform our merchants of potential security risks, ensure equipment, software and processes on campus are compliant with PCI standards and better protect our customer cardholder data.