CUSP (CU I&E) Submission: Web-Based PCI Data Security Standard Assessment [1]

The Office of the Treasurer centrally oversees the bank and credit card accounts for all campuses and units of the University of Colorado. On a yearly basis, the university's bank, Wells Fargo Bank, requires the University of Colorado to submit a document confirming that all credit card merchant accounts across the university, 147 as of July 31, 2012, are in compliance with the Payment Card Industry Data Security Standard (PCIDSS).

"The PCI Data Security Standard was developed by the Card Associations (Visa®, MasterCard®, Discover® Network, American Express and JCB) to help protect Cardholder information. It sets comprehensive requirements to assist businesses in securing their information network, as well as in establishing and maintaining procedures and policies to prevent threats and unauthorized access to their systems and applications. The consequences and costs of non-compliance and of a data compromise can be devastating for any merchant. While businesses who are not PCI DSS compliant risk losing their ability to process card payments, they are also very likely to lose customer confidence and revenues in case of a compromise and will potentially face fines, penalties and expenses to repair the damages done."

Over the past few years, different methods have been utilized by the Office of the Treasurer to assess and confirm that each campus and system department accepting credit cards is compliant under this standard. Initially, paper self-assessment questionnaires (SAQ) introduced by the PCIDSS council were distributed to each department; they were printed, completed manually, signed and sent back to Treasury for review, and then filed. It was an extremely time intensive process for all. For the 2010 cycle, the university engaged a local compliance firm called Coalfire Systems, Inc., which supported an online portal called Navis for these self-assessment questionnaires. The advantages of this portal were: accessibility via internet, navigation tools to determine correct version of the SAQ, and ability of Treasury to see progress and assist departments to answer questions. The disadvantages of this portal were: expense, slow navigation, problems with password resets, and multiple documentation upload requirements.

In the summer of 2011, a committee of CU system staff began meeting to determine if the university could customize a similar website portal to allow merchants to complete the self-assessment questionnaire without the drawbacks of the Navis portal.

A SharePoint site was set up on the University Information Systems (UIS) server which served as the online portal for the navigation and document upload. The Office of the Treasurer provided the list of account names and numbers, contact names and e-mail addresses for each department required to fill out the online self-assessment questionnaire; there were approximately 140 departments uploaded into the SharePoint site. In addition, the self-assessment questionnaire from the PCI Council was reformatted from a word document

into an excel spreadsheet to allow departmental staff to automatically identify which version of the SAQ they should complete. Campus training sessions were held on each campus to demonstrate the portal and documents, and give staff a “heads up” on the new site.

HOW DOES THIS IMPACT THE UNIVERSITY?

The process was overwhelmingly successful! It saved the university over $25,000 in the first year, was easier for the departmental staff to access the site and upload required compliance and policy documentation, and was more efficient for the Office of the Treasurer. UIS was available to reset passwords, a task that demanded much Treasury staff time in the previous cycle. Staff could get to their accounts and the portal was easy for them to use. Treasury staff could easily see which departments had not completed the SAQ and were able to answer questions and assist staff who were confused about which version to complete. UIS periodically sent Treasury a report, noting the accounts that had not been activated, and if they had, when the site was last used; this assisted Treasury staff to follow up with departments which had not started the process. At the end of the compliance cycle, 100% of departments had completed the SAQ.
Based on feedback from campus staff and IT campus security teams, the portal was easier to understand, documentation uploads were less cumbersome, and the entire process less confusing. Campus departmental staff are also pleased to know that they will not have to learn another process for next year’s cycle. The committee will continue to meet to incorporate suggestions, refine the portal, and use what they learned to improve the overall method.

IMPLEMENTATION STATUS

The PCI compliance process was implemented for the 2011-12 cycle and will be used for future cycles.

Submitted by: Joe Tinucci, Assistant Treasurer and project lead, Chirag Joshi, Assistant Chief Information Security Officer, Sean Myers, Service Operations Manager, and Lexie Kelly, Assistant to the Treasurer

Groups audience:
Controller

Links
[1] https://www.cu.edu/controller/cusp-submission-web-based-pci-data-security-standard-assessment