Trustwave®
Smart security on demand

Higher Education and Payment Card Industry Compliance: Challenges and Actions

This industry brief provides an overview of challenges that higher educational institutions face when addressing Payment Card Industry (PCI) compliance requirements, as well as key recommendations for addressing those challenges.

THE PROBLEM

As discoveries in science and technology occur, people continue to look to the universities for progress. State and federal funds go to universities to pursue discovery—the next cure, the faster processor, the smaller CPU. And if the universities don't deliver, the people expect them to educate the people that will.

Unfortunately, in the realm of data security, people are, understandably, losing faith in higher education institutions. In the past year, breaches at U.S. universities may have exposed millions of Social Security numbers and bank account numbers. A university can no longer wait to protect its students, faculty and employees.

BULGING RISK INVENTORY

A wealth of personal information already resides on university servers—Social Security numbers, grades, health records, etc. And, as universities continue to add a variety of payment options (on or offline) they're dealing with more and more payment card information. This proliferation of payment card acceptance at universities adds yet another item to their already bulging risk inventory, and puts the institutions into scope for the PCI Data Security Standard (PCI DSS).

The PCI DSS is a framework for developing a robust payment card data security process created and maintained by the PCI Security Standards Council. The Council's five founding global payment brands—American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. —incorporate the PCI DSS as the technical requirements of each of their data security compliance programs.

OUTSIDE THE TRADITIONAL MERCHANT MODEL

When considering the organizations that fall in to the scope of PCI DSS, many people think of large retailers or large volume e-commerce merchants; higher education institutions don't quite fit the traditional merchant mold. For instance, to encourage and maintain the free exchange of ideas, they commit themselves to open networks. Payment processing systems are often spread over a large geographical area; universities often utilize multiple IT departments that may not coordinate.

Higher education institutions also depend on frequently less-than-satisfactory state and federal funding that demotes data security to the bottom of many priority lists. In addition, they have a great many "merchants" accepting payment cards on their campuses—bookstores, hospitals, parking services, pre-paid campus cards, athletic departments, alumni organizations, and housing and food services, among others. While a number of departments accept payment cards on behalf of the university, it's likely the institution itself has one contract with its acquiring bank (the bank that credits a merchant's account for their payment card receipts or "batch")— the merchant agreement.

DECENTRALIZED PROCESSING IS AN IMPEDIMENT

Unfortunately, the above scenario often results in a decentralized processing system. In some cases, departments/merchants request their own merchant ID (an acquirer-assigned number used to identify an entity that accepts payment cards; for purposes of reporting, processing and billing) directly from the institution's bank, leaving the university's financial management staff in the dark. In other cases, some departments may have hundreds of IDs from the university's block of merchant IDs assigned by its acquiring bank, but only use two. This decentralization prevents an institution from knowing where cardholder data resides on their servers—perhaps the greatest obstacle to PCI DSS compliance. If an institution does not know where an asset is located, they cannot protect it. And without central oversight, departments may think of PCI DSS compliance as an IT or finance issue, when in reality it is the responsibility of every department.

Without a centrally managed merchant ID system, an institution may not have a full grasp of which of their departments actually accept payment cards, let alone whether or not they're PCI DSS compliant. Without a thorough understanding of their entire payment card environment, an institution cannot compare its practices to the PCI DSS, or even know where to implement PCI DSS compliant policies, procedures and technology.

In reality, PCI DSS compliance is the entire institution's responsibility with duties and accountability assigned at every level of the payment process. Decentralized acceptance of card payment can lead to relationships with multiple third party vendors, making it difficult to create and enforce the policies and procedures necessary to maintaining PCI DSS compliance. Any institution that does not implement a PCI DSS compliance program with central oversight and enforcement will find the process difficult, if not impossible.

RECOMMENDED ACTIONS

Security breaches in the university environment are almost a weekly occurrence. These breaches impact universities just as they do corporations, despite occurring outside the corporate mold. A university's commitment to open networks, multiple merchants under one merchant agreement, and reliance on outside funding for resources all add complexity to the compliance process. Below are some best practices to consider when developing a PCI Compliance Program at your higher educational institution.

DEVELOP A PLAN

Any university entity looking to start a program aimed at PCI DSS compliance needs a realistic plan. Ideally, this plan would first call for enlisting the cooperation of its upper management by setting up an introductory meeting with the appropriate individuals. The costs of non-compliance should be laid out in detail with special emphasis on the necessity of upper management's support in gaining the cooperation of the entire university. The project manager should also meet with IT and finance departments to fully explain the project and their corresponding roles and responsibilities. The next step involves contacting all remaining personnel to effect the necessary "culture shift" towards compliance. This effort will explain the process in appropriate detail, emphasize upper management support, and inform those more directly affected of their responsibilities.

IDENTIFY ALL PAYMENT ACTIVITY

At the next stage, during assessment meetings, the goal is to identify all e-commerce activity within the institution, as well as understand how that e-commerce and payment card acceptance is conducted by each "merchant." If applicable, involved parties need to determine which departments hold merchant IDs. If resources allow, a scan of the environment should be conducted to ensure all systems are

identified and included. This scan can be performed in-house, or by a Qualified Data Security Company (QDSC). Based on information gathered from the assessment stage, PCI compliant policies and procedures can be created for all departments that accept, or plan to accept, payment cards or conduct ecommerce.

Ideally, this process involves working with the IT department to create a network architecture that segments the environment, cordoning off sensitive information from systems that remain accessible to all. At this point, third parties engaged in the university's acceptance of payment cards should be closely examined and renewed or changed as necessary.

TRAIN DEPARTMENTS AND EMPLOYEES

Finally, a training and education program for all departments and employees involved in payment card acceptance should be designed and implemented. This program should aim to lay out specific roles and responsibilities for employees and departments, and make them aware of any resources available should they have any questions or concerns.

GOAL: COMPLIANCE AND PROTECTION OF KEY ASSETS

If an institution of higher education wishes to accept payment cards, they must comply with the PCI DSS. The standard is based on best data security practices, and as such will go a long way to protect all other critical assets. PCI DSS compliance mitigates risk, protects universities from the costs of a breach, and hardens their overall security stance. When a university complies with the PCI DSS, they not only protect themselves, but also their lifeblood—their students and employees.