How the PCI DSS has Impacted Institutions of Higher Education

It has been many years since the Card Associations and Acquiring Banks have stepped up enforcement of the Payment Card Industry Data Security Standard (PCI DSS) within the Higher Education sector. However, while the number of incidents has gone down, compliance within this sector continues to be problematic. The lack of compliance persists because their environment presents a number of challenges that are not prevalent in a normal merchant environment.

Understanding the Higher Ed Environment

Higher education establishments have certain traits in common: they have a culture of openness (i.e. information is to be shared) and function much like a city unto themselves, which means they are many types of organizations/merchants rolled into one. For example, most higher education establishments have at least one or more of the following:

- Bursar (Cashier) Office
- Police Department
- Medical Facilities (hospitals/ clinics)
- Café's / Restaurants
- QSR's
- Housing / Dining
- Performing Arts (ticketing and concessions)
- Athletic Facilities (ticketing and concessions)
- School Bookstore
- Post Office
- School Clubs
- Conferences / Event Registration

As a result, the compliance program at a higher education establishment must manage the compliance of multiple merchant accounts, much like an acquirer or ISO. The difference is that, unlike that acquirer/ISO program, the Higher Ed compliance manager often has a limited ability to enforce their mandate. This disconnect is due to the independent nature and distributed power structure of the business units/departments within a higher education organization. Depending on their structure, some higher education organizations are in a better position to tackle this issue than others.

To better understand the challenges higher education entities face, they are divided into four categories:

Small to Medium Private

Single campus/location where all activities run through a single administrative structure. Faculty and staff report to one executive who reports to the board of regents/ trustees. This means both IT and the business office report to the same executive as the faculty. Information technology and control of business related activities are centralized.

Large Private

Limited campuses/locations where activities run through multiple administrative structures. Each structure has its own executive who functions in a relatively autonomous environment. These executives all report to one executive who reports to the board of regents/trustees. Most have centralized IT and administrative functions, but they typically act as support for employees that are embedded in another business unit and do not have direct oversight of the personnel in the business lines executing these functions.

Small to Medium Public

Limited campuses/locations where activities run through multiple administrative structures. Each structure has its own executive who functions in a relatively autonomous environment. These executives all report to one executive who reports to the board of regents/trustees. Most have centralized IT and administrative functions, but they typically act as support for employees who are embedded in another business unit and do not have direct oversight of the personnel in the business lines executing these functions.

Large Public

Numerous campuses/ locations with multiple administrative structures. Each structure has a chief executive who functions in a relatively autonomous environment, but ultimately reports to a centralized campus administrator. All campuses are governed by an oversight body (board of regents). The campus executive manages numerous business units that also operate in a relatively autonomous fashion. These campuses typically have centralized IT, finance, and compliance functions, but these units often support the personnel that are embedded in the business lines and do not have direct oversight of the personnel in these business lines.

It is easy to see that higher education organizations have a fundamental problem implementing their PCI DSS Compliance program because the people in charge of the program have very limited authority over the people who must abide by it. This is further complicated by the independent nature of higher education personnel, who typically resent being told what to do and which vendors to use.

The Hub and Spoke Model

The Hub and Spoke model is very popular with large private and most public higher education establishments because it emulates their existing structure. In this model the creation of the PCI DSS validation program typically resides with either the Bursar or Controllers[1] office. They train staff within the departments that have merchant accounts on the PCI DSS and its compliance validation procedures. These staff members are then required to complete self-assessments and report their status to the central office that in turn manages the relationship with their acquiring bank[2]. If remediation is required, the business unit provides the central office with a remediation plan and updates them on their progress on a regular basis. The central office then aggregates this data and updates the acquirer on the progress of the overall organization.

Centralized PCI DSS Compliance Management

Centralization of credit card processing and compliance oversight has typically been relegated to smaller private organizations; however, this trend has reversed over the past few years and larger private and smaller public higher education organizations are increasingly implementing this type of program. In the centralized model, all merchant accounts must be approved by the bursar/ controller. In addition, all

[1] While Information Technology is a key player in PCI DSS compliance, it is rarely in charge of oversight of institutions PCI DSS compliance validation program.

[2] In rare cases the department/ business unit owns their own merchant account and communicates directly with the acquiring bank, this is not a good practice and should be highly discouraged.

payment processing technology must comply with guidelines set by the bursar/ controller's office. Compliance is validated by an independent party within the institution (usually internal audit) and remediation projects are overseen by the bursar/ controller as well. As with the Hub and Spoke model, communication with the acquirer is managed by the bursar/ controller or through a centralized support office such as Treasury.

The Period of "Painful Learnings"

In the mid to late 2000s, the higher education community went through a period of "painful learnings" in which most higher education organizations incurred at least one (usually multiple) information security events. Some of the most common mistakes in this period resulted from:

- Liberal access rights to systems that contained cardholder data (lack of network segmentation)
- Improper storage of cardholder data
- Use of non-PA DSS validated applications
- Use of non-compliant service providers
- Non-sufficient data asset inventory / classification[3]

Change is in the Wind

As a result of this period of "painful learnings" many higher education organizations are implementing centralized PCI DSS compliance validation programs as well as incorporating some of the following best practices:

- Implementation of proper network segmentation and asset control
- Mandating the use of PA DSS validated payment applications
- Mandating the use of PCI DSS validated service providers
- Utilization of tokenization and encryption
- Outsourcing transaction processing to compliant third parties
- Centralized management of the acquirer relationship on behalf of all merchants

Another key factor contributing to the rise in higher education PA DSS compliance is the emergence of the PCI SSC Internal Security assessor (ISA) program. This program enables compliance and technology professionals at higher education facilities to receive the training needed to better manage their environment and assist their colleagues with the design and implementation of more secure payment processes.

[3] Not knowing where cardholder data resides