

Higher Education and PCI Compliance: Definitions, Challenges, and Actions

The Problem

The general public holds higher education institutions to a high standard in the realm of science and technology. As discoveries in science and technology continue to amaze, 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, as the newspapers attest, in the realm of data security, the people are, understandably, losing faith in higher education institutions. In the past year, reports say that hackers invaded more than 29 college or university networks in the United States, and one independent report estimates that up to 30 percent of data security breaches reported in the media last year took place at a college or university.¹ A university can no longer wait to protect its students, professor and employees.

A wealth of personal information already resides on university servers—Social Security numbers, grades, health records, etc. But, as universities continue to add a variety of payment options (on or off-line), they're dealing with more and more payment card information. This proliferation of payment card acceptance at universities adds yet another item to an institution's already bulging risk inventory, as well as puts them into scope for the Payment Card Industry's Data Security Standard (PCI DSS). A symposium held in May 2006 by the Treasury Institute for Higher Education discussed the PCI DSS, its relation to higher education institutions and the challenges universities face when implementing a compliance program. This paper includes a great deal of information presented at that two day workshop (for more information, please see the PCI DSS Symposium link in the "Resources" section found at the end of this paper).

Prior to 2004, to assure consumers of their brands' reputations as trustworthy payment options, each of the major card associations (Visa, MasterCard, American Express and Discover) drew up individual data security programs they required merchants to follow in order to accept their card brand. As one might imagine, the process of ensuring compliance with four different, yet equally complex, security regulation methods proved impossible for many merchants. To simplify the process, in December 2004 Visa and MasterCard aligned their security standards—Visa's Cardholder Information Security Program (CISP) and MasterCard's Site Data Protection Program (SDP) —and announced the creation of the PCI DSS. Since its creation, both American Express and Discover have accepted the standard as well.

When considering the PCI DSS's scope, 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. With payment processing systems, many times, spread over a large geographical area; universities

¹ Doan, Lynn. "College Door Ajar for Online Criminals." *Los Angeles Times* 30 May 2006. 5 June 2006 <<http://www.latimes.com/technology/la-me-hacks30may30,0,1085392.story?coll=la-home-headlines>>.

often utilize multiple IT departments that may not coordinate. Higher education institutions also depend on often 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.

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 others; from the university’s block of merchant IDs assigned by its acquiring bank, some departments may have as many as 12, but only use two. This decentralization prevents an institution from knowing where cardholder data resides on their servers—perhaps the greatest obstacle to PCI 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 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 compliant. Without a thorough understanding of their entire payment card environment, an institution can not compare its practices to the PCI DSS, or even know where to implement PCI compliant policies, procedures and technology.

In reality, PCI 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 compliance. In addition, after a statistical analysis of its 2005 digital forensics investigations, AmbironTrustWave found that 60 percent of compromises were due to third party error. It’s important to remember that a breach in just one department could possibly hinder the entire institution’s ability to accept payment cards at all. Any institution that does not implement a PCI compliance program with central oversight and enforcement will find the process difficult, if not impossible.

Understanding PCI

Preventing data security attacks is not a simple issue to address for any organization, higher education or otherwise. Organizations with a stake in the flow of electronic commerce respond to threats in a variety of ways. As mentioned above, all major credit card brands, including American Express and Discover, now endorse the PCI DSS. The card brands require that *all* merchants and service providers that

store, transmit or process credit card holder information comply with the PCI standard.

The PCI-DSS consists of 12 requirements in pursuit of six goals:

- **Building and Maintaining a Secure Network**
 1. Install and maintain a firewall configuration to protect data
 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protecting Cardholder Data**
 3. Protect stored data
 4. Encrypt transmission of cardholder data and sensitive information across public networks
- **Maintaining a Vulnerability Management Program**
 5. Use and regularly update anti-virus software
 6. Develop and maintain secure systems and applications
- **Implementing Strong Access Control Measures**
 7. Restrict access to data by business need-to-know
 8. Assign a unique ID to each person with computer access
 9. Restrict physical access to cardholder data
- **Regularly Monitoring and Testing Networks**
 10. Track and monitor all access to network resources and cardholder data
 11. Regularly test security systems and processes
- **Maintaining an Information Security Policy**
 12. Maintain a policy that addresses information security

Depending on an institution's payment card transaction volume, the card associations may require it to validate PCI compliance through on-site assessments performed on a recurring basis by an approved independent third-party assessor. While merchant (Table 1.1) and service provider (Table 1.2) level definitions may vary slightly among the card brands, most defer to Visa's definitions:

Table 1.1

Level	Merchant Classification Criteria (as of July 18, 2006)
1	Visa & MasterCard: Any merchant- regardless of acceptance channel -that: <ul style="list-style-type: none"> ▪ Processes over 6 million Visa or MasterCard transactions per year ▪ Has suffered a hack or an attack that resulted in an account data compromise ▪ Visa or MasterCard determines should meet the Level 1 merchant requirements ▪ Has been identified by any other payment card brand as Level 1
	AMEX: Any merchant- regardless of acceptance channel -that processes over 2.5 million AMEX transactions
2	Visa: Any merchant- regardless of acceptance channel -that processes 1 million to 6 million Visa transactions
	MasterCard: Any merchant that processes 150,000 to 6 million MasterCard e-commerce transactions
	AMEX: Any merchant- regardless of acceptance channel -that processes 50,000 to 2.5 million AMEX transactions
3	Visa: Any merchant that processes 20,000 to 1 million Visa e-commerce transactions
	MasterCard: Any merchant that processes 20,000 to 150,000 MasterCard e-commerce transactions
	AMEX: Any merchant- regardless of acceptance channel -that processes less than 50,000 AMEX transactions
4	Visa: Any merchant that processes fewer than 20,000 Visa e-commerce transactions or processes fewer than 1 million Visa transactions
	MasterCard: Any merchant that processes fewer than 20,000 MasterCard e-commerce transactions and less than 6 million MasterCard transactions

Table 1.2

Service Provider Level	Selection Criteria
1	All VisaNET processors (Member and nonmember) and all payment gateways
2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually
3	Any service provider that is not in Level 1 and stores, processes, or transmits less than 1,000,000 Visa accounts/transactions annually

Table 1.3

Merchant Level	Validation Actions	Validated By	Deadline
1	Annual On-site PCI Data Security Assessment and Quarterly Network Scan	Qualified Data Security Company or Internal Audit if signed by Officer of the company Qualified Independent Scan Vendor	9/30/04 New level 1 merchants have up to one year from identification to validate
			AMEX: 10/31/06
2	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Merchant Qualified Independent Scan Vendor	New level 2 merchants: 9/30/07
			AMEX: 10/31/06
3	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Merchant Qualified Independent Scan Vendor	6/30/05
			AMEX: Recommended 10/31/06 ***AMEX will establish mandatory date in 2007***
4	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Merchant Qualified Independent Scan Vendor	Validation requirements and dates are determined by the merchant's acquirer

Table 1.4

Service Provider Level	Validation Actions	Validated By	Deadline
1	Annual On-Site PCI Data Security Assessment and Quarterly Network Scan	Qualified Data Security Company Qualified	9/30/04
		Independent Scan Vendor	
2	Annual On-Site PCI Data Security Assessment and Quarterly Network Scan	Qualified Data Security Company Qualified	9/30/04
		Independent Scan Vendor	
3	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Service Provider	9/30/04
		Quarterly Network Scan	

Where a university lies within this framework is not exactly clear. The institution may hold one merchant agreement or contract with their acquiring bank, however, a number of merchant IDs that accept payment cards exist beneath that agreement. Whether the card associations and acquiring banks look to the entire institution's volume of transactions or look at the volume of transactions for each separate business unit, or merchant ID, and assign each a corresponding merchant level (i.e., one level one merchant vs. nine level four merchants) depends on the bank and card association concerned.

During a panel discussion at the aforementioned symposium mentioned in the introduction of this paper, representatives from Visa, American Express, Discover and one acquiring bank answered questions about where universities fit in the merchant levels scheme. The consensus was that ultimately it's the acquiring bank's responsibility to identify a university's merchant level, unless otherwise identified by the card associations. The acquiring bank representative said that it depends on the university's merchant agreement with their bank. If they have one merchant agreement and all card payments from various departments roll into that one agreement, that aggregate total of transactions would be used to determine merchant level. Whereas if separate university departments have separate merchant agreements with the acquiring bank, each separate department would be considered separately regarding their transaction volume and merchant level. Because American Express and Discover are themselves both card brands and acquirers, they also examine the merchant agreement to determine merchant levels.

Roles and Responsibilities

Card Associations

As the authors and enforcers of the PCI DSS, the card associations hold the highest position of power in the process, however with power comes responsibility, including:

- Ensuring the standard is current and relevant to new technologies and attack methods
- Examining the effects on merchants implementing the standard
 - Making implementation of the standard feasible
- Ensuring the standard is clearly written and understandable
- Resolving confusion over interpretation of the standard
- Defining merchant levels and validation expectations
- Determining fines in the event of a breach

Acquiring Banks

Because it's nearly impossible for the card associations to contact every merchant and ensure they comply with the PCI DSS, ultimately, it's the acquiring banks that administrate PCI compliance. The card associations stipulate that acquiring banks mandate merchant compliance with the PCI DSS. In the event of a breach, the associations issue fines directly to the acquiring banks (though an acquiring bank's contract with a merchant normally holds the merchant liable should a breach occur).

Acquiring banks' responsibilities include:

- Negotiating merchant agreements

- Informing their merchants of the PCI DSS
 - Determining merchants' levels
 - Validation requirements
- Clearly defining liability in the event of a breach

Merchants

The 12 requirements themselves remain the responsibility of the merchant. While the card associations created them, merchants must implement the policies, procedures and technologies they need to achieve compliance. The card associations issue fines to the acquiring bank, the acquirer's contract with a merchant will generally specify that the merchant is liable should a data security breach be traced back to their place of business. Costs of the investigation, remediation, card re-issuance, and fines therefore, all fall to the merchant.

A merchant's responsibilities include:

- Meeting the requirements of the PCI DSS
- Requiring by contract that engaged third parties meet all PCI security standards
 - Understanding what processors those third parties use
- Completing the PCI Self-Assessment Questionnaire, *if required*
- Hiring a Qualified Independent Scan Vendor, *if required*
- Engaging a qualified outside assessor if necessary
- Protecting other confidential information

Auditors and Assessors

A level one merchant may not have the necessary resources to hire or dedicate a full-time compliance staff to perform an audit. They must therefore engage a Qualified Data Security Company (QDSC) to perform an on-site audit of their environment. If identified as a level one, two or three merchant; a Qualified Independent Scan Vendor must complete their required quarterly network scan. All QDSCs are certified by the card associations, work directly with the merchant, and submit documentation and questions directly to the acquiring bank or card associations on the merchant's behalf. The PCI DSS is daunting to any merchant, and the majority will want to utilize the expertise of a qualified assessor to help them through the questionnaire, point out vulnerabilities, make remediation suggestions or provide other data security information. However, in the event of a breach, the compromised merchant is obliged to undergo a complete forensics investigation conducted by a QDSC.

An assessor is responsible for:

- Developing in-depth knowledge of the PCI DSS requirements
- Understanding the card associations' interpretation of the standard
- Validation Documentation—including Report on Compliance (ROC)
- Keeping current on industry best practices
- Conducting quarterly and annual network scans and penetration tests

Best Practices

Developing an adequate compliance program takes time, and convincing an entire university population that it's in their best interest, takes even more. However,

taking the initiative to begin a compliance program is the hardest part, and once taken, the progress is often swift and in the end, worth the effort. The best practices explained below come from real world examples of what universities have found helped them most on their journey toward compliance. The practices outlined below are only a general overview and should not be relied upon without careful consideration and review with a qualified data security expert.

Buy-in

At first glance it would seem only the finance and IT departments are concerned with PCI compliance, however, the entire university needs to get involved. Without assistance from every department that accepts payment cards, a compliance manager won't know where information is located in their infrastructure, be able to enforce the necessary policies and procedures, or secure the resources required to even get the program started. The compliance manager should facilitate "buy-in" across all departments by convincing upper-management (the Board of Regents, controllers, etc.) that their participation is crucial in convincing others of the importance of PCI compliance.

An institution can achieve buy-in in a number of ways:

- Gather relevant information to present to upper management
 - Articles/Headlines discussing university breaches
 - Liability costs
 - *Reputation*
 - *Fines*
 - *Card Re-Issuance fees*
 - *Forensic investigation costs*
 - *Costs of notifying victims*
 - *Remediation costs*
- Create a full-time position to manage compliance or assign a compliance-project manager
 - Shows an institution takes compliance seriously
 - Employee should report regularly on progress and issues to upper-management representative
 - Develop communication campaign to inform and engage departments
- Form an e-commerce review board
 - Should include Treasury office, Office of Information Technology, Legal
 - Review department requests for e-commerce capabilities
 - Review departmental progress towards/maintenance of PCI compliance
- Create an administrative e-commerce guide
 - Explains university e-commerce policies and procedures
 - Explains importance of PCI DSS and the university's compliance policies
- Send a letter explaining the PCI DSS and the university's expectations
 - Sent to department heads/business managers
 - Identify stakeholders
 - Inform stakeholders that PCI DSS is their responsibility
 - Explain consequences of non-compliance
 - *Shut down of e-commerce site by management if non-compliant*
 - *Fines if breached*
 - *Department on their own if breached*

In the beginning, it's most important to identify the stakeholders in any compliance project. As harsh as it may seem, these individuals must be responsible, and held accountable, for non-participation. This paves the way for open dialogue with upper management to answer any questions, and helps keep the program on course.

Assessment

With the decentralization of merchant ID management prevalent in the university environment, a compliance manager may find it difficult to ascertain exactly how payment card or other confidential information enters their network, or where it resides once it's there. This determination is the fundamental first step to compliance

It is just as important to define what an institution is NOT responsible for. For example; if a department conducts e-commerce, but uses a separate provider to actually take, transmit and store cardholder information, that department's PCI obligations may decrease significantly (assuming the provider has signed the necessary third party agreement). Any compliant payment processes currently in use should be explored as possible solutions for all departments. With an understanding of processes currently in place a manager can more easily assist departments in implementing the changes required.

To conduct an introductory assessment, a compliance-project manager should:

- Make department heads accountable for their network infrastructure
- Meet with department heads to ascertain who is within scope of the assessment
- Understand e-commerce solutions currently in use
- Examine IP addresses and merchant IDs to confirm e-commerce merchants
- Hire an outside assessor if necessary
 - Provides unbiased feedback from a Visa-qualified data security professional
- Weigh risks and rewards of certain departments using e-commerce
 - For example, a student group selling t-shirts for a one-time event, is there a more appropriate payment option?

While only a starting point, these meetings emphasize that the university's commitment to PCI compliance is real, and that it expects the same commitment from its individual departments. This is similar to, and a logical continuation of the buy-in step detailed above. Network architectures can be complex, and it may be more realistic for larger universities to hire an outside assessor to complete this step.

Segmentation

Universities thrive on the collision of ideas—one idea challenging another. To foster this environment, ideas must flow freely. This is just one way universities differ from traditional merchants with regard to PCI compliance. Whereas an e-commerce retailer can restrict access to their network and lock-down everything on a need-to-know basis, universities have a special interest in keeping networks as open as possible. PCI compliance, and the strong access control measures contained in the standard, do not fundamentally conflict with open networks. The PCI DSS only requires that organizations place strict access control measures on payment card information.

To support open networks, but also secure assets, a compliance program should:

- Call for segmentation within the environment

- Continue open access to university resources
 - *Libraries, interest groups, etc.*
- Separate critical assets
 - *Payment card information, Social Security numbers, grades, etc.*
- Restrict access to segments that contain cardholder and other confidential information
 - Need-to-know basis
 - Build boundaries around segments (firewalls, IDS/IPS, etc.)

A university, like a city, has a wealth of resources it wants to make available. For example; a city has a library that it wants open to all residents. To decrease the risk of stolen media material, the city hires a security guard to watch the front door; but for the most part access to the library is unrestricted as the assets are non-critical. However, the city also has critical assets. These are kept in a bank, under lock and key with access granted only to certain authorized individuals. In this way ALL assets are treated in a way appropriate to their importance or relevance.

Third Parties

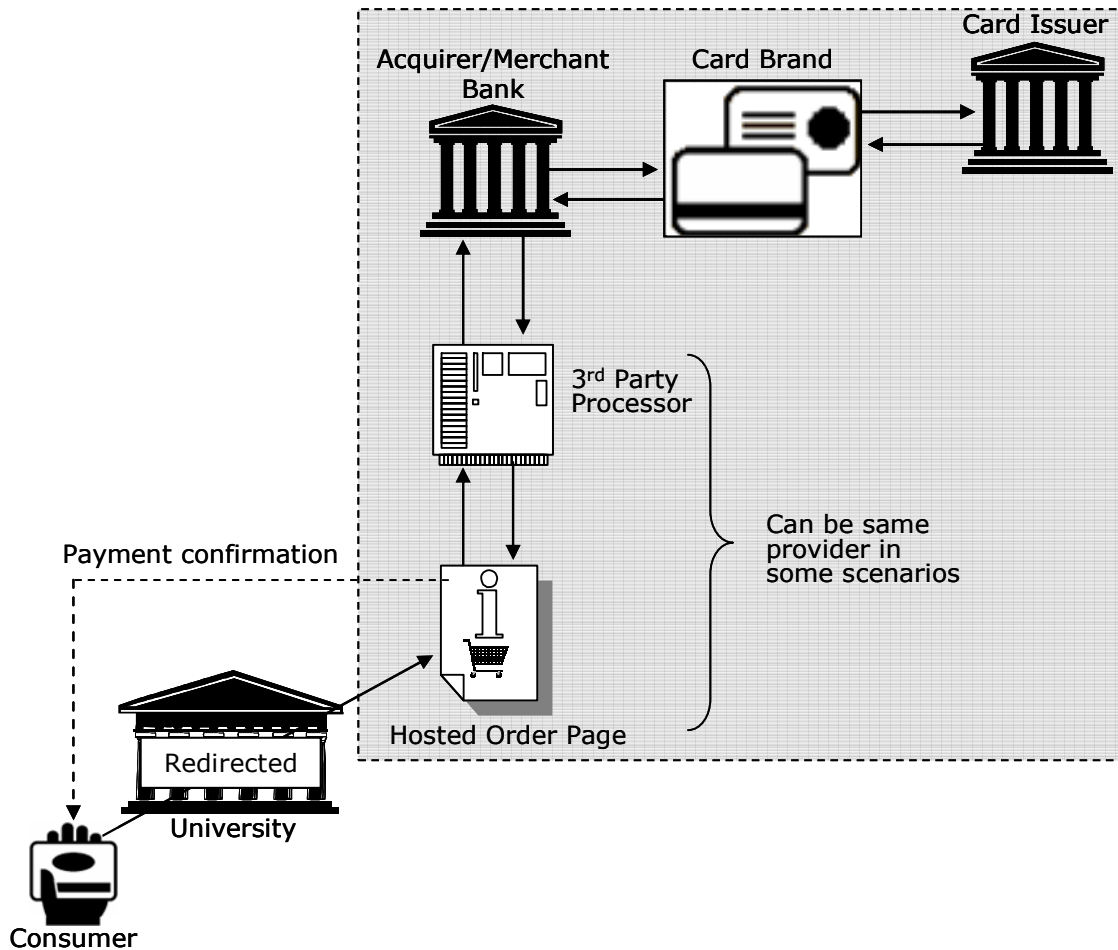
A number of university athletic departments use a third party vendor (such as Paciolan, tickets.com or Ticketmaster) for automated ticket sales. This vendor allows the upload of events, seating charts and pricing. A sports fan will visit their favorite university sports team's site and click on a link for tickets. The site then sends them to the vendor's online shopping cart. The vendor then handles all payment transactions, completely separate from the university's Web site and network infrastructure. This is just one example, but when accepting payment cards, more likely than not, at some point in the process a university uses a third party. As mentioned above, more than half of all data security breaches occur due to third party error. In any payment card environment, it's imperative to know what third parties are performing what services and that their services comply with the PCI DSS.

When using a third party's products or services, an institution must:

- Ensure the party signs a third party agreement
 - Require that they meet all PCI security standards
 - Specifically assigning liability in the event of a breach
- If using a payment application, ensure the application follows Visa's Payment Application Best Practices (PABP)

A university may find it best to completely outsource their e-commerce solution so that their network does not transmit, process, or store cardholder data (illustrated below in diagram 1.1). In this arrangement, a cardholder visits a university site or online storefront, which redirects them to a third party site (a HOP or Hosted Order Page provided by vendors such as CyberSource, First Data or RBSLynk) to facilitate the transaction. This does not exempt the university from PCI compliance; they still must ensure that the security posture of the server that redirects cardholders to another site is compliant. They must also sign a third party agreement with the HOP provider stipulating that the provider will handle cardholder data in a PCI compliant manner. This third party agreement requirement does not apply only to HOP configurations. Depending on the payment card environment, any number of third party vendors can be involved—increasing the risk.

Diagram 1.1



Training

While the PCI DSS may seem mostly a technical standard, in the end, employees are the first line of defense, or the first failure point. In order to follow PCI compliant policies and procedures, they must understand where they apply, and how to follow them. They also need education on the proper use and implementation of technology within the environment. Any environment is only as secure as its weakest link and many times—due to ignorance, human error, or malicious intent—that link is an organization’s members.

Any compliance program should include yearly training sessions for staff that address:

- The PCI DSS and importance of compliance
- The university’s policies and procedures
- Accepting payment cards
- Requesting a merchant ID
- Consequences should an employee or department fail to follow written policies

- The incident response plan
- Resources for those using or starting e-commerce

PCI compliance, and risk management in general, is not a one-time event. It's cyclical, and constant reassessment is necessary for any entity to stay informed of and mitigate risk. Continuing education affirms this best practice and keeps PCI compliance at the top of the institution's priority list.

Conclusion

Security breaches in the university environment are almost a weekly occurrence. These breaches impact universities just as they do corporations, despite their lying 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. The best practices outlined in this paper are ideals, or what would be implemented with unlimited resources, but depending on available funding, some steps may involve more time or customization.

Any entity looking to start a program aimed at PCI 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.

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 accounted for. 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 currently (or with plans to) accept payment cards or conduct e-commerce. 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.

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.

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 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.

Resources

The Treasury Institute for Higher Education's PCI DSS Symposium

- <http://www.treasuryinstitute.org/welcome/modules.php?name=News&file=article&sid=45>

Visa Cardholder Information Security Program

- http://www.usa.visa.com/business/accepting_visops_risk_management/cisp.html?it=wb||Learn%20More

American Express Data Security Operating Procedures (DSOP)

- http://www125.americanexpress.com/merchant/oam/ns/USEng/FrontServlet?request_type=navigate&page=dataSecurityRequirements

Discover Information Security and Compliance (DISC)

- http://www.discovernetwork.com/resources/data/data_security.html