Ensuring Your Institution Meets the PCI Security Standards

Compliance is crucial to prevent gaps in data security

A University Business Web Seminar Digest | Originally presented March 2016

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and to facilitate the broad adoption of consistent data security measures globally. Despite the PCI DSS, information breaches continue to leave colleges and universities with unrecoverable damages as a result of undetected exposure within their compliance and prevention programs.

These reputation-damaging data security gaps leave the institution without a defensible position when confronted by auditors, regulators, litigators, and insurance claims. In this web seminar, an industry expert discussed the recent updates to the PCI DSS, why data breaches continue to occur on campuses, and what you need to do to ensure compliance at your institution.

Ron King
President and Chief Operating Officer, CampusGuard

PCI security standards are managed by the PCI Security Standards Council, and they affect all merchants and service providers. Nelnet Campus Commerce is a Level 1 Service Provider, so they have a very rigorous certification process. And of the 352 companies that are globally qualified security assessors, CampusGuard is the only one that's focused solely on higher education.

You are responsible for safeguarding the credit card data at your institution and complying with the PCI DSS. In your Merchant Agreement with your acquiring bank, it states that you are responsible for adhering to and being compliant with their security standard, and also with the PCI DSS.

Over the past several years, I've been looking at statistics regarding where breaches are coming from. Compared to all other sectors, higher education has a disproportionate share. The other thing that's shocking is that approximately 50 percent of the breaches occurring in higher education are a direct result of hacking. By comparison, the total number of hacking breaches among retailers is under 20 percent.

So, higher education is unfortunately a prime target for hackers. Most of the breaches—starting with hacking and then continuing with fraudulent use of credit card information—come about because of very simple things that could be fixed. When a university reports its compliance, they are either omitting important pieces altogether or are not defining scope completely. They are also looking at compliance as a one day a year check-off event, and they have an incomplete risk management strategy instead of a continuous strategy.

Across campus, you may have somewhere between five and 100 different locations taking cards in every conceivable way—for tuition and fees, parking, dining, residence halls, theater, athletic ticketing, concessions, and so on. Compare that with McDonald's, which has 15,000 stores but one very simple, very secure way of accepting credit card payments. This is the major reason why it's so difficult for a college or university to be compliant with the data security standard.

“ Most of the breaches… come about because of very simple things that could be fixed.”

- Ron King, President and Chief Operating Officer, Campus Guard

High stakes for compliance

There are many obstacles to PCI compliance and data security in higher education. You have open networks and systems because the culture of higher education has been to keep information available to all at any time. But one of the key reasons for breaches is lack of proper scope definition, which is a very complex discussion at a college or university. Despite overloaded staffs and fiscal constraints, PCI compliance is mandatory. If you take cards in any form or fashion, then PCI applies to you. And it’s pass or fail—you are compliant or you are not. At the end of the day, compliance with PCI DSS is just addressing best practices. If you do the right thing and put the controls in place, you will be compliant.

If you do have a breach, it is going to change your life. Those on campus who have responsible positions will see their job descriptions change for the next year or so after a breach, and you’ll lose a lot of productivity. In addition to responding to the banks and to your QSAs, etc., you will also be responsible for responding to state laws requiring notification of any breach of personally identifiable information.

Then you also potentially have fines and penalties. If you have a major breach, you will get notified initially through your bank that you have been identified as a Common Point of Compromise, or CPOC—four letters you never want after your name. Depending on the nature of the breach, each of the card brands could fine you $500,000 to begin with. Then you have the costs associated with notifying all potential victims, confirmed victims, card replacements, and card fund losses. You also have to consider the costs associated with setting up a phone bank to respond to questions, etc. On top of all that, the biggest problem is reputation. It’s priceless. You are going to have all kinds of questions there. You just don’t want to go through that headache.

The PCI DSS is now relatively mature, with tweaks applied to address current threat landscapes and trending attacks causing compromises. The change in v3.2 is technical in nature. While SSL and TLS were the gold standards for encrypting traffic across the internet, they now have been found to be vulnerable.

Importance of staying vigilant

If you do have a compromise, you need to respond immediately. The PCI DSS is a minimum standard for security. For example, the standard says you should patch a published vulnerability within 30 days, but good security practice says you should apply the patch as soon as you are notified.

Review the changes in your environment. You are going to have personnel changes—people will move in and move out of your department. You also have the responsibility of training. Put the policies in front of them to read and sign. Hold a periodic review with your teams to make sure the right controls are in place. Review hardware and software technology changes. They are evolving. There’s point-to-point encryption, and deep conversations about mobile payments. All of these need to be thought of and addressed.

You may never be asked by your bank to show proof of compliance, but you still have the responsibility because you signed a merchant agreement. Even if the bank has never given you any guidance, you still need to be compliant. If you have a breach and it’s bad enough for the bank to get involved, the bank will wash their hands of it and say, “Well, here’s the agreement. You said you’d be compliant at all times.”

What about Chip and Pin? It actually has nothing to do with PCI compliance. It is a bank issue related to shifting the liability from fraud to merchants. October 2015 was the date for everyone to switch to the Chip and Pin. But it does not protect the information—data sent out is not encrypted. The chip is actually a little computer that generates a special three-digit code for a particular transaction that can never be used again, preventing fraudulent or counterfeit credit cards. But that has nothing to do with PCI compliance.