What’s happening on campus?

CampusGuard Visit July 25th & 26th

Ed Ko, our Qualified Security Assessor (QSA) from CampusGuard, visited Binghamton University last month. The review went well as we continue to make progress towards achieving compliance. As expected, Ed stressed the need to deploy Point to Point Encryption (P2PE). Implementing P2PE at specific merchant departments is really the final piece to our compliance puzzle. These departments include Campus Recreation, the Anderson Center Box Office, and the Events Center Ticketing Office.

PCI DSS Compliance Training 2016

All but 40 employees have completed training thus far. Thanks to all of you who have done so. Please note, the training module is NOT on the WeComply website. So if you have completed modules like Haz/Com and all the others found on WeComply, PCI DSS was not one of them. You can only find the PCI training module on Blackboard. To access it, please visit the following web site and follow the instructions:

http://www.binghamton.edu/revenue-accounting/pci_dss/training.html

Remember, Binghamton University cannot achieve PCI compliance unless everyone is properly trained on an annual basis. So your cooperation in this endeavor is greatly appreciated.

RFP 16/17/004

A Request for Proposal was released on August 2nd seeking a vendor to provide Binghamton University with a comprehensive eCommerce software. Once this new software is implemented, many of our campus merchants will immediately benefit from the software’s ability to integrate with the point of sale software they are using now. On the accounting side, the software will integrate with Banner in real time. Many other departments that currently do not take payments, will be able to do so in a PCI compliant manner.

Did you know?

P2PE is a registered trademark of the Payment Card Industry Security Standards Council (PCI SSC).

However, many vendors claim to offer P2PE even though their solution is not validated by the council.

Nevada is the only state to require its merchants to comply with the PCI DSS by state law.
Outstanding Compliance Issues

1. **Annual Training** - there are still 40 employees that need to complete training. Please ensure that everyone in your department is trained. Reminders will be sent out and continue until training is completed.

2. Many Attestations of Compliance (AOCs) from third parties have expired, and a few have never been obtained. If a third party collects payments on our behalf, we must ensure that company is PCI compliant. In addition, all contracts with third parties must contain PCI language. The proper language will make it easier to obtain the annual AOC.

If you have questions, please contact Steve Duseau. sduseau@binghamton.edu

---

**P2PE: How it works and why it will help BU**

Point to point encryption (P2PE) is a payment security solution that immediately makes cardholder data indecipherable at the moment the card is swiped. The card swipe is also known as the point of interaction (POI). From the POI, the encrypted, indecipherable codes, are sent to the credit card gateway or processor for decryption. The keys for encryption and decryption are never available to the merchant, meaning that the merchant’s equipment never sees the 16 digit credit card number. (Known as PAN, or primary account number, within the PCI DSS). According to the DSS, full PAN must be present in order for the PCI DSS to apply. The end result is that the merchant’s equipment is removed from the scope of the PCI DSS because full PAN is not present within the merchant’s system. In order to truly experience P2PE, the process described above must be validated by the PCI Security Standards Council (PCI SSC). Solutions that employ similar technology, but are not validated, are technically not P2PE. Currently, P2PE is hardware dependent. This means that the card swipe terminal, or POI device, must also be validated by the council in addition to the encryption/decryption solution itself. Merchants who are using a validated P2PE solution and attest compliance by using a Self Assessment Questionnaire (SAQ), are eligible to complete SAQ P2PE-HW. This SAQ contains only 35 questions. It is likely the merchant’s environment was subject to SAQ C (157 questions) or perhaps even SAQ D (329 questions) prior to the implementation of a validated P2PE solution. The significant change in questions required is indicative of the PCI scope reduction achieved through P2PE. Merchants save significant time and money as the PCI requirements they must comply with are greatly reduced. At the same time, security is significantly enhanced because the encryption greatly reduces the risk of credit card fraud.

---

**Scam using PayPal’s “Money Request” Feature**

Cyber criminals are sending people phishing emails and taking over their PayPal accounts. Once they have control, they send people bogus money requests through PayPal. However, to make things worse, they include a personal message which leads to a Trojan that could steal your banking information. So, remember to always Think Before You Click, even if the email gives every appearance of coming from legitimate, trusted sources.