What’s happening on campus?

Cyber Liability Insurance

Binghamton University has been researching the purchase of a cyber liability insurance policy. Such a policy would help protect our campus from the losses that would result from an information breach, whether through cyber attacks or human error, such as a lost or stolen device containing sensitive information. This insurance is tied to our PCI DSS Compliance. Campuses that are PCI compliant will receive a considerable discount on premiums for this insurance. Conversely, campuses found to be severely lacking in the area of PCI Compliance may not be able to obtain cyber liability insurance at all. So, while achieving and maintaining compliance with the DSS has always been very important, this additional factor makes it even more so.

Compliance Audit

SUNY Oneonta was selected by the Office of the State Comptroller to be the first campus audited for PCI Compliance. The OSC will continue to audit other campuses moving forward. So please make certain that your department achieves and maintains compliance as Binghamton University could be selected for audit at some point in the near future.

2015 CampusGuard Visit Report

Ed Ko, our Qualified Security Assessor (QSA), from CampusGuard visited BU August 3rd-5th. His report from this visit was disseminated to all campus merchant departments on Friday, October 2nd. Please follow Ed’s guidance to ensure compliance for your department.

Did you know?

October is National Cyber Security Awareness Month. Many banks are emphasizing security awareness this month and sending information on the topic to their customers. 


Remember to have all PCI trained employees sign and date the Training Acknowledgement document.
Outstanding Compliance Issue

For almost every campus merchant department that is currently not compliant, missing or incomplete documentation is the key issue that needs to be addressed. The following documents are most frequently the cause:
1. Terminal Inspection Log
2. CDE Visitor Log
3. Signed Training Acknowledgement
4. Attestations of Compliance (AOCs)
5. Not having addressed one or more of the above documents in department policies and procedures.
6. Not having defined your department’s CDE or CDEs in the policies and procedures document.

If you have documentation questions, please contact Steve Duseau.

Human Error

A recent study has shown that human error is the leading contributor to data breaches. This is why annual PCI compliance training and clearly defined departmental procedures is so important. The study also found that the most frequent example of human error was a “failure to follow policies and procedures.” While it’s true that our employees can be our greatest weakness when it comes to data security, well trained and vigilant employees are also our greatest strength. To read the full article that reported on this study, use the following link:

The Liability Shift associated with EMV

A change that is putting new credit cards in many Americans’ wallets will also shift billions of dollars of card-fraud liability to retailers from big banks. Merchants are scrambling to deal with the end of a longtime policy in which financial institutions absorbed the cost of certain fraudulent credit-and-debit card transactions. Starting October 1st, the merchants will have to foot the bill for the transactions if they haven’t upgraded their payment terminals to accept new, more secure cards. For millions of U.S. consumers, the new cards being rolled out are replacing the familiar action of swiping a card with dipping it at the cash register. After the change, consumers in most cases will still not be liable for fraudulent transactions on their cards. Behind the scenes, though, the risks of card fraud are shifting. Under timetables announced by card networks Visa Inc. and MasterCard Inc., most card issuers starting October 1st are expected to immediately start passing certain fraudulent transaction costs onto retailers that don’t have the capability to process the chip-based cards, industry executives said. The move from the old cards with the magnetic stripe on the back to the new ones with an embedded computer chip is aimed at reducing fraud with counterfeit cards. Historically, card issuers such as banks and credit unions covered those costs. The new chip cards, which have been flooding consumer mailboxes for months, provide a unique code for each transaction, compared with static data that are contained on the traditional magnetic strip. While the chip itself won’t stop thieves from hacking a merchant’s payment system, any stolen card information will be virtually useless since the data change each time it is used. Some of the nation’s largest merchants have already switched to the upgraded terminals, which should shield them from the new liability. Wal-Mart Stores Inc., Home Depot Inc. and Target Corp. are among the big retailers that have already been processing chip-card transactions.

Excerpted from an article by Robin Sidel of The Wall Street Journal, for the full article see http://on.wsj.com/1LQyqyc