Did you know?

A credit card swipe terminal with Point to Point Encryption (P2PE) would have thwarted last year’s breach at Target stores. But card holder data (CHD) was being transmitted in clear text between the swipe terminals and the cash registers at Target making it easy for cyber thieves to steal the data.

Please send your department’s written procedure for credit card processing to Steve Duseau, sduseau@binghamton.edu

CampusGuard Visit

Ed Ko, our Qualified Security Assessor (QSA), from CampusGuard visited Binghamton University on Monday and Tuesday, November 24th and 25th. There was quite a bit accomplished in the area of PCI Compliance over those two days.

Ed began by giving a presentation on the PCI DSS and what it means for all of us at BU. The workshop was attended by 38 employees representing more than a dozen different campus departments. On day two, Ed met with the senior officers group and the deans bringing an enhanced awareness of this important issue to the leaders of the university.

During the two day visit, Ed also met with 11 departments on campus that accept credit card payments. As a university, we have improved greatly since our first visit from CG in 2010. But there is always room for improvement and we must always remain vigilant to protect card holder data. Here are some highlights of things we learned from the visit:

- Point to Point Encryption (P2PE) and chip and pin technology will greatly enhance the security of card holder data. We will be reaching out to merchant departments beginning in 2015 to assist in upgrading their credit card terminals to devices that employ chip and pin technology.

- The use of a third party is a good way to limit the scope of the PCI DSS. However, it is important that liability limiting language be a part of any third party contract. Also, third party vendors must provide an attestation of compliance (AOC) annually. See page two for more on both of these issues.

- Each department was asked if they had a written policy and procedure for the acceptance of payment cards. Please send your department’s procedure to Steve Duseau (sduseau@binghamton.edu) for review. Thank you to those departments that have already done this.

- Each department was also asked if they took annual PCI DSS Compliance training. While each department replied "yes", it should be noted that about 30 employees across almost all departments have not completed the training for 2014. If even one employee fails to complete this training, then we as a university are not compliant with the PCI DSS. It is noteworthy that President Stenger and many of the senior officers have completed the training module. If they can make time in their busy schedules for the module, then we all can.
More on Third Party Contracts

All contracts with third party vendors should contain liability limiting language in which the vendor accepts responsibility for compliance with the PCI DSS. An addendum should be added to current contracts not containing this language.

In addition to the contractual language, vendors must provide an attestation of compliance (AOC) annually. Currently, many of our vendors provide us with a “certificate of compliance” or a “certificate of a successful scan”. Unfortunately, neither one of these documents qualifies as an AOC. The proper document can be found at the Payment Card Industry Security Standards Council (PCI SSC) web site.

The only exception to the AOC rule is that if the vendor can be found on the Visa Global Registry of Service Providers, then an AOC from that vendor is not necessary.

Links to both the PCI SSC and Visa web sites can be found on the Revenue Accounting web page. A link to that page is on the right.

PCI DSS Web Page

Please visit the PCI DSS section of the Revenue Accounting Department’s web page for information on the PCI DSS.

http://www.binghamton.edu/revenue-accounting/pcidss.html

Myths and Misconceptions

1. One Vendor and Product will make us compliant
2. Outsourcing card processing makes us compliant
3. PCI Compliance is an IT project
4. PCI DSS will make us secure
5. PCI is unreasonable; it requires too much
6. PCI requires us to hire a Qualified Security Assessor (QSA)
7. We don't process enough credit card transactions to worry about compliance
8. We completed a SAQ for our department, so we are compliant
9. PCI makes us store card holder data
10. The PCI DSS is just too difficult

Cardholder data (CHD) sent through Email

Accepting cardholder data via email or other messaging systems (chat, text, instant messaging, etc.) is not permitted at any time. The corrective action is to reject the message and notify the submitter that the information cannot be accepted in this manner. Do not process the transaction and delete the email from your inbox and from your trash folder.