What’s happening on campus?

CampusGuard Visit—A Big Success!

Ed Ko, our QSA from CampusGuard, visited BU on Wednesday, January 31st through Friday, February 2nd. Ed visited almost all campus merchants. He did assess all merchant IDs associated with the university’s acquiring bank. For the first time, since originally consulting with CampusGuard in 2010, the university was found to be 100% compliant with the PCI DSS! It was a long road, but we got there together. Thank you to all the employees at our campus merchant departments whose dedication to this effort made this achievement possible. Now we must maintain our compliance.

Ed also reported that he has been promoted to a Director level position at CampusGuard. While I was happy for him, I was disappointed to learn that this will result in Ed being phased out as our QSA. Our new QSA will be Jeff Burt, who reports to Ed.

Attempted Breach

During the week of May 14th, Cornell University experienced an attempted breach of their credit card terminals. The following was reported by a Director at Cornell: “An individual identifying herself as working for the Discover Riviera Group entered multiple retail units wanting to test our credit card readers with a few “low dollar amount transactions with multiple credit cards that would be declined.” She had what appeared to be appropriate ID, but no business card that she could leave. She was very convincing and persistent. We reported this to Freedom Pay (our Credit Card processor) and they said that we were the second university to contact them this week with visitors from the same “Discover” group. To everyone’s knowledge, Discover does not have teams of people testing credit cards on university campuses. Please be aware and let your staff know that this is a hoax. Both universities involved are sending equipment to Freedom Pay so they can test for skimmers/keystroke loggers. We didn’t see any outward evidence of tampering with the two units that were touched at Cornell University, but we’re taking the “better be safe than sorry” approach.”

If any person, other than the PCI Compliance Officer or our QSA, wants to “test” or inspect a credit card terminal, please report the incident immediately. If such a person is on campus, call the University Police immediately. Then report the incident to the PCI Incident Response Team (PCI IRT). This can be done by email to: pci-security-incident@binghamton.edu

You can also call the PCI Compliance Officer (7-3214), the Director of Risk Management and Administrative Compliance (7-6660), or the CISO (7-6198) as these three positions make up the PCI IRT.

Also, for security purposes, please verify the accuracy of your advertising at least monthly. Make certain that phone numbers, mailing addresses, and all other contact information that a customer may use is accurate on your web page, mailings, and anywhere else that it may be advertised to potential customers. If you find inaccurate contact information has been provided to customers, please report it as a PCI incident.
Annual Compliance Maintenance Issues

I. Annual Training - Well over 100 employees have already completed their training this year. Thank you very much to those who have. For BU to MAINTAIN compliance in 2018, we need everyone to participate.

II. An Attestation of Compliance (AoC) is needed from your third party vendor UNLESS that company appears on the Visa Global Registry of Service Providers. In that case, please take a screen shot of the listing from the Visa web site and place it in your department’s folder on the shared drive. If you need to know which document is needed, check the past newsletters or ask Steve Duseau. Again, to MAINTAIN compliance we MUST have these REQUIRED documents from third parties.

Compliance (and Security) Across Many Standards by CampusGuard

Campus-based organizations like resorts, colleges and universities, and medical facilities host a vast amount of financial, medical, and personal information, which makes them an attractive target for hackers looking to steal data. For every guest, student, or patient, there is a social security number, bank account number, credit card number, etc. waiting to be harvested. In fact, the 2017 Verizon Data Breach Incident Report (DBIR) stated that, of all the documented breaches worldwide 92% impacted hospitality, 81% impacted healthcare, and 67% impacted education. Just take a look at some of the data breach stories detailed below and you can easily validate why security measures are needed.

A recent article in University Business magazine revealed that colleges and universities estimate their current compliance costs to range from 7 to 11 percent of total campus operating expenses, bringing the total reported annual cost of compliance in higher education to approximately $27 billion.

So how do you successfully wrap your arms around the varying standards and requirements you are obligated to comply with? Start by defining and then implementing a comprehensive security framework that covers multiple requirements. That framework can then be augmented when new standards come out (think GDPR) rather than spinning up an entirely new program to address the new requirements each time.