What's happening on campus?

**PCI DSS Compliance Training 2016**

More than 100 employees have completed training thus far. Thanks to all of you who have done so. However, almost 200 still need to complete the required training. To do so, 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.

**Point to Point Encryption (P2PE) update**

We are pursuing P2PE solutions for the Events Center Ticketing office, the Anderson Center Box office, Campus Recreation and any other merchant location where it can increase security and reduce PCI scope. Since P2PE is a relatively new technology, we have experienced many challenges in this endeavor. Some PCI validated P2PE solutions are not integrated with the software that we currently use on campus. In addition, several software vendors that we currently use have already contracted with specific P2PE solution providers. These providers are not necessarily able to connect to our bank and they want BU to sign legal agreements. Those agreements contain language that is neither acceptable to our QSA nor university counsel. However, in spite of these challenges, we will establish mutually beneficial relationships with vendors and P2PE providers in order to install P2PE where it is needed on campus.

**Did you know?**

Cyber-criminals collected $209 million in the first quarter of 2016 by extorting businesses and institutions to unlock computer servers. At that rate, ransomware is on pace to be a $1 billion a year crime.
Outstanding Compliance Issues

1. Annual Training - there are still almost 200 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

Multi-Factor Authentication Heads PCI's List of Changes

By David Heun

Multi-factor authentication will be required for administrative access to card data and systems for Payment Card Industry data security compliance this week. The PCI Security Standards council will deliver its 3.2 data security standard version, effective April 28, strengthening rules for data access, providing criteria for ongoing compliance programs, and reminding merchants and network operators to continue to migrate to a more secure Web protocol, or Transport Layer Security. The PCI DSS 3.1 version will expire Oct. 31, 2016. The multi-factor requirement is the biggest change in the PCI DSS 3.2, said PCI chief technology officer Troy Leach. Authorization may include a password, a token or smartcard and some form of biometrics, Leach said in a recent blog post. Previous PCI requirements call for two-factor authentication, but the new rule of multi-factor makes it consistent that "at least two credentials" are used for access, Leach said. "A password alone is not enough to verify the user's identity and grant access to sensitive information," Leach said. This new requirement applies even if the individual seeking access is within a trusted network, or if the person seeking access works internally or as a third party, he added. PCI recommends that organizations review how they manage access to their cardholder data environment and review the current administrator roles to identify where the new requirement will require changes to authentication.

For the full article go to this link: http://www.paymentssource.com/news/retail-acquiring/multi-factor-authentication-heads-pcis-list-of-changes-3023992-1.html

Death of Musician Prince

Last week, news broke that Prince Rogers Nelson was found dead in his home in Minneapolis at age 57. Internet criminals are going to exploit this celebrity death in a number of ways, so be careful with anything related to Price's death: emails, attachments, any social media (especially Facebook), texts on your phone, anything. There will be a number of scams related to this, so Think Before You Click! (Similar scams occurred when Robin Williams passed away in 2014)

Also, with the recent earthquakes in Ecuador and Japan, there are charity scams sticking up their ugly heads. If you want to make donations, go to your favorite charity by opening your browser and type their link in the address bar. Do not click on any links in emails.