What’s happening on campus?

PCI DSS Compliance Training 2016

PCI DSS Compliance training for 2016 was released on Monday morning, February 29th. There are now three options for completing training:

1. Complete the WeComply training module
2. Pass a revalidation quiz
3. Complete training in a classroom setting

Explanations of each option can be found here:
http://www.binghamton.edu/revenue-accounting/pci_dss/training.html

This is also the web page all trainees should navigate to in order to commence computer based training.

Completion of any one of the training options satisfies the annual training requirement. 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.

Did you know?

Approximately 91% of successful data breaches started with a spear phishing attack. Be aware of emails that you do not recognize and do not click on any links within such emails.

Please complete annual compliance training as soon as possible. Thank you!
Outstanding Compliance Issue
Third Party Contract Management

For merchant departments that are not compliant at this time, the number one issue has to do with third party contracts. Many departments need an Attestation of Compliance (AOC) from their third party service provider. Either we do not have an AOC on file or the AOC we do have has now expired. Some departments do not have liability limiting language in the contract that they have with their third party vendor. The language recommended by Campus-Guard can be found here:

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

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

Five damaging data breaches caused by human error
By Lewis Morgan

Each time a data breach hits the news, certain sections of the media jump on their hacking hobbyhorse in a frenzy of excitement, frothing hysterically about cyber war and desperate to pin every attack on China, North Korea or Russia – usually in spite of a manifest lack of evidence that these countries are in any way culpable. “Was it China? I think it was China.” “No. WAIT! North Korea! It’s got to be them.” Although the idea of a group of state-sponsored criminal hackers working in an abandoned nuclear bunker in China (all moody lighting and walls festooned with flat-screen monitors displaying code in scrolling green columns like The Matrix) makes hacking sound sexy, it’s usually just Dave in marketing’s fault for downloading a bank statement emailed to him by a bank that the company doesn’t even have an account with. Human error is the cause of most data breaches. It’s no secret that the largest threat to an organisation’s data is its own employees – whether deliberate or not. In fact, some of the most damaging data breaches have been caused by human error. Here are five particularly egregious examples.

Facebook reveals dates of birth of 80,000,000 users
Clinic leaks HIV status of patients
Pentagon suffers data breach via spear phishing attack
Sony hackers used phishing emails to breach company networks
Ubiquiti fraud: the $46 million cyber crime

For more information about each of the five examples above, view the full article here:
http://www.itgovernance.co.uk/blog/five-damaging-data-breaches-caused-by-human-error/

RANSOMWARE

Ransomware is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a trojan, whose payload is disguised as a seemingly legitimate file. Payment is virtually always the goal, and the victim is coerced into paying for the ransomware to be removed, which may or may not actually occur, either by supplying a program that can decrypt the files, or by sending an unlock code that undoes the payload’s changes. A key element in making ransomware work for the attacker is a convenient untraceable payment system. A range of such payment methods have been used, including: wire transfer, premium-rate text messages, online payment voucher service such as Ukash or Paysafecard, and the digital currency Bitcoin.  