Information Security Office
Administrative Department Review
2018-2019 Report

Due: 05.31.2019

Report submitted annually.
Data and analysis from three annual Reports will inform a new Plan.

6b. Procedure, Measurement Tool and Timeline
1) **Goal**: Reduce risk of College server and network appliance compromise, while focusing on the highest priorities based upon the weighted risk scores from our College's vulnerability assessment software. **Activities performed to accomplish outcome(s):** Monitored monthly risk assessment reports from the College's vulnerability assessment software. Success is measured by a 'risk rating' that comprises common vulnerabilities and exposures (CVE) risk score, known exploits in the wild for each CVE, and Metasploit Modules for each CVE. Monthly reports track risk increase. Deprecated servers, particularly on premise Banner servers were archived and powered down to reduce risk. Data references include CVE score, known published exploits, and Metasploit Modules. **2) Goal**: Provide quality information security training to departments across the campus to reduce network account compromises due to phishing and malware victimization. **Activities performed to accomplish outcome(s):** Contact department directors and request invite to department monthly meeting (or any other preferred method) to perform information security training to that department. Yearly enhancements of PowerPoint used for training keeps training relevant and directly applicable to the College's staff. Success is measured by quantity of at-risk departments trained – in this case 17/24 for this year. Tools used include an Excel spreadsheet to track training status for departments, PowerPoint of training content, and research of myriad cyber-security training sources. Data is gathered as training status is updated (monthly). 3) **Goal**: Reduce risk of College owned confidential information being breached by a business partner which would impact the community's confidence and trust in the College by ensuring that they follow industry standard best practices for information security principles as well as maintaining compliance requirements such as SOC-2, PCI, HIPAA, FERPA, ISO 27001 or others as appropriate. **Activities performed to accomplish outcome(s):** Performed information security assurance evaluations of new vendors who either transport, store, or process COCC confidential or restricted data. Evaluations include AIM, CollegeNet R25, SecureLink, RevelSystems, Fire-Engine-Red, Ink-Me, and Ellucian Banner Cloud. Tools were email, phone calls with vendors, SOC-II and COCC's custom vendor evaluation and compliance reports. Evaluations occur once a vendor has completed the RFP process and/or is a likely

candidate as a business partner for the College, although data is gathered at year-end for this report.

4) **Goal**: Keep the campus community abreast of current cybersecurity topics by producing a monthly newsletter.

   Activities performed to accomplish outcome(s): Created 12 newsletters focused on relevant information security topics for the College. Archive of newsletters is located on the intranet under the CIO / Information Security Office site.

5) **Goal**: Maintain the College's PCI compliance.

   Activities performed to accomplish outcome(s): Performed yearly PCI compliance attestation using the assessment software provided by the College's payment processor. Perform scans of the COCC network via the College's payment processor. I measured success by the fact that the College was PCI compliant (as stated on PCIComplianceManager (which TouchNet uses to measure and monitor PCI compliance for its customers). No data references are used other than our PCI compliance (we are compliant until Dec 2019). Data gathered quarterly as PCI compliance network scan notices were received from the vendor.

6) **Goal**: Reduce risk of insider threat, which can be either accidental or intentional, by maintaining access to network files as defined by the 'Need to Know' best practice.

   Activities performed to accomplish outcome(s): Review N:\ drive permissions for incorrect user permissions. (Often when one employee leaves a department, they will retain permission to the network folder for a short time, often for training purposes, and these permissions are overlooked for cleanup at the time.) This past year there were roughly 75 permissions entries to be corrected, however several are tied together (one user having access to several individual subfolders). Success is slightly arbitrary for this outcome, as finding zero incorrect permissions would be best, however finding and resolving incorrect permissions is considered a benefit. I perform this work using Varonis DatAdvantage.

7) **Goal**: Monitor and manage endpoint virus/malware attacks against the College.

   Activities performed to accomplish outcome(s): Log into the College's enterprise antivirus console (SEM) daily and remediate any malware that was not automatically cleaned up by the SEM. Daily reports monitor daily productivity. Yearly reports indicate that between July 1 2018 and today's date, May 31rst, 27 Viruses/spyware and 1382 adware/PUA were cleaned. Data was gathered daily regarding malware to be cleaned, and yearly for total malware resolved.

8) **Goal**: Reduce risk of leaked confidential information that can result in fines, lawsuits, or diminished community trust in the College.

   Activities performed to accomplish outcome(s): By constantly monitoring myriad information security news sources and studying penetration testing, I develop skills to assess our College's security posture. Success was determined by identifying 10 unique vulnerabilities for the College and working with IT staff to resolve those vulnerabilities or mitigate them to an acceptable level. Tools used include anything that white-hat or black-hat hackers would use such as nmap, Metasploit, kali Linux, sslyze, smbclient, and the list goes on. Assessments happened weekly as new tools identified that could assess potential vulnerabilities. This office was able to determine the following potential risks or improvements:
   1) Use PSF records to stop criminals from spoofing COCC email accounts.
   2) Physically destroyed old Banner sun disks.
   3) Purchased and implemented technology to DOD-Wipe SATA and SAS drives.
   4) Browser back-button cached credentials flaw in Ellucian Banner cloud.
   5) SSL3 used on ldap.ad.cocc.edu:636
   6) Barry and I evaluated and resolved issues with unencrypted COCC ID# for Dynamic Forms.
   7) Old cipher (md5) used for LDAP TLS configuration.
   8) Allow of executables in archive files if canned properly with AV
   9) Request that the college post notification in the email body: [EXTERNAL EMAIL]
   10) Unquoted Service Path PrivEsc in IntelliAdmin <=5.6

9) **Goal**: Focus on professional improvement, keeping abreast of the ever-shifting cyber security landscape.

   Activities performed to accomplish outcome(s): Currently studying for OSCP utilizing lab and at-home course training. Utilizing roughly 3-5 work-hours and 8-12 home-hours per week. Plan to test September 2019. Extracurricular courses include Python, BASH scripting, assembly debugging, exploit research, and much more. No data to gather towards this however have completed roughly 50% of the at-home course and have compromised 5 or the 30 lab machines. This studying also counts towards CPE hours for my existing CISSP training. On track to obtain OSCP certification 2019 or 2020 at the latest.

7. Data

The following data has been gathered about the Information Security Office's Effectiveness:

1) Collected risk assessment data about the Colleges on premise servers ranks our College consistently around 900K, across approximately 110 end-points. Risk grows slightly, but steadily.
2) College PCI compliance was 100% this year.

3) This office produced newsletters for each month of the academic year. These reports are being added to the InfoSec Intranet site this week.
4) This department identified roughly 75 incorrect permission sets with collaboration from other department personnel.
5) This department cleaned 27 viruses/spyware and 1382 adware/PUA between July 1rst and 05.31.2019.
6) This office, in collaborative effort with other departments, identified and resolved or remediated to acceptable levels ten unique security vulnerabilities.
7) This office maintained the CISSP certification standing by performing 40 hours of CPE study, and progressed through half of the OSCP certification self-study lab work.
8) Information Security Training performed for roughly 17/24 departments deemed at-risk for confidential data loss via phishing or malware exploits. This will be improved on (see below.)

8. Summary and Analysis: Continuous Improvement
(Report-to be completed annually when data are available)

Data suggests that this department is adept at finding and resolving/mitigating risk. The quantity if new, unique risks identified is extremely encouraging. This office set out to identify 10 unique issues and was able to do so. Many of these newly identified risks were the result of studying for the OSCP certification, which reaffirms that hands-on certification training (OSCP) is a strong addition to the high-level certification (CISSP.)

PCI Compliance has improved this year, due to the improved due-diligence of this office and better tools for PCI compliance and reporting from TouchNet. PCI Compliance this year was better than the previous year, where we were non-compliant for a month due to lack of notification about attestation report problems from the vendor.

Information compliance training requires improvement. Scheduling issues are a problem at times, and this office has plans to create online training that will be available to departments and employees where scheduling conflicts occur. Once complete, a series of 3 to 5 videos will be available for those personnel or departments who cannot attend trainings in person. Monthly newsletters provide training to help fill in the gaps in employee knowledge about InfoSec topics and shows due-diligence should the College ever find itself under scrutiny for an employee involved information security incident.

Our College's CIO has already approved evaluation of MalwareBytes and Nexpose Insight that could potentially help close the gap on malware risk. These two tools working in tandem would both help block incidents prior to happening and also mitigate / remediate incidents that did occur.

Evaluation of new business partners shows due-diligence by the College and helps ensure confidential data stays protected. This office is proving quite effective in these evaluations and is proud of the preemptive information security assurance it provides with these evaluations.

Our College's endpoint management software has improved, thus making this office's efforts more fruitful. There were no large-scale malware replications this year, unlike previous years where small issues with zero-day malware replication occurred.

In summation: This office feels that there can be improvements made towards the in-person information security awareness training, and that the addition of online video training will help immensely. This office is building even more skill sets in vulnerability detection and analysis that will complement a solid foundation of overall information security practices. Malware remediation time is at an all-time low. The potential addition of endpoint malware defense software and SIEM applications might provide significant improvement for those two challenges. Strong support from the rest of the IT staff and the CIO help this department succeed in both incident prevention and remediation.