Information Security Office
Administrative Department Review
2017-2018 Plan

Department Overview	
Administrative Department	Information Security Office
Contact (Person responsible for reporting)	Wesley Dymond
Participants	Wesley Dymond
Date Review submitted	May 31, 2019
Report Submitted to	Dan Cecchini and Julie Hood Gonsalves

1. Mission Fulfillment

Information Security Office Mission Statement:

The Information Security Office (ISO) works with the campus community to reduce threats against confidential College information by ingraining information security best practices into the College's technical infrastructure, governance, business processes and mindset.

2. Department Purpose

Information Security Office Vision Statement:

Expand and improve upon a comprehensive security posture, while ensuring secure access to information for those who need it to perform their jobs. A three-fold strategic approach accomplishes this: an appropriate governance and policy structure; affordable security architecture and solutions; and a holistic security awareness program that addresses staff, faculty, and the community at large.

3. Department Strengths

Education: Holds the Certified Information Security System's Practitioner certification. One of 84,500 practitioners in the US with this gold-standard information security management certification. Also, have Masters of Science degree for Information Security Management with a focus on Security Engineering.

Work experience: Having worked previously as a mainframe and network admin, am capable of understanding the technologies associated with IT administration, networking, data storage, data processing, transmission, and more. This allows me to help translate security concerns to technology terms for faster resolution. Similarly, work experience plus Higher Ed helps bridge the language and vernacular differences between business administration and information security administration. Able to find the balance between security and usability.

4. Department Challenges

There are gaps in this office's tools and resources that if closed, would enhance this office's capabilities to detect and resolve issues. For instance, a security information event management (SIEM) product would provide a dashboard of our technology infrastructure, indicate where malware or system breaches begin and provide a roadmap as malware or compromises spread from resource to resource.

Emergency management of phishing campaigns or malware attempting to spread across the College, which sometimes takes days to resolve, frequently interrupts project work.

Switching between administrative and technical tasks can slow down project completion due to the time required to refocus on complex projects and technical issues.

Scheduling training with other departments can be challenging, particularly with the high level of College employee staff who have vacations and <12 month contracts. Training with departments at monthly meetings works best, however gaps in employee training still occur.

5. Department Goals→Department Outcomes

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.

   Outcome: By analyzing monthly reports, assist the technology owners by identifying and describing the vulnerabilities true threat and risk to the College.

2) **Goal**: Provide quality information security training to departments across the campus to reduce network account compromises due to phishing and malware victimization.

   Outcome: The ISO will present information security training to all departments that process confidential information in digital or physical form. This office will also provide

training to all other departments upon request or as opportunities arise.

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.

   Outcome: The ISO will evaluate the security posture of all existing and future College business partners that store or process College confidential information, documenting the results as a standardized process, reporting yearly the list of business partners evaluated and the evaluation results.

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

   Outcome: Publish 12 monthly newsletters (July – June) to the Bobcat Community public folder.

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

   Outcome: Perform yearly PCI compliance attestations using the assessment software provided by the College's payment processor. Perform scans of the COCC network via the College's payment processor's network scanning software as required for PCI compliance.

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.

   Outcome: Reduce College risk by identifying and correcting all inappropriate file/folder access permissions as documented by an annual review of each department's network folder(s).

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

   Outcome: Remove network endpoint malware infections in a timely manner one business day,) reducing risk of compromise of the College's networks or confidential information.

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

   Outcome: College risk will be reduced by discovering 10 unique vulnerabilities, whether they be technical, administrative, or physical, and working to resolving or mitigating those risks to a level accepted by the College.

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

Outcome: Obtain one cybersecurity certification (CEH, CISM), become affluent in one cybersecurity technology (Python, Wi-Fi cracking), and maintain existing certifications (CISSP).

6a. 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.

Procedure / Activity: Ensure that the enterprise vulnerability assessments are completed.

Measurement Tool: Monthly automated reports from the enterprise vulnerability assessment application.

Timeline: This automated process occurs monthly. Ongoing enhancements include adding new end-points when they are stood-up on the network.

2) Goal: Provide quality information security training to departments across the campus to reduce network account compromises due to phishing and malware victimization.

Procedure / Activity: PowerPoint presentation discussing applicable information security training followed by a Q&A session.

Measurement Tool: Number of required departments trained, number of non-required departments trained.

Timeline: Yearly.

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.

Procedure / Activity: Evaluate all COCC business partners that receive, process, or store confidential or restricted from the College.

Measurement Tool: Quantity of new COCC business partners evaluated and deemed as compliant.

Timeline: Yearly.

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

   Procedure / Activity: Develop a monthly newsletter using MS Publisher.

   Measurement Tool: Quantity of newsletters created.

   Timeline: Newsletters published monthly, reporting is yearly.

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

   Procedure / Activity: Perform 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.

   Measurement Tool: Percentage of months the College was PCI compliant.

   Timeline: Reporting is yearly. Compliance evaluation and attestation is yearly; compliance scans of our network are quarterly.

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.

   Procedure / Activity: Meet with a representative from all departments that process confidential information in digital form, and evaluate network permissions for folders that could potentially contain confidential or restricted information.

   Measurement Tool: Quantity of incorrect permissions found. (Less is better because there was less initial risk; more shows greater risk reduction. It is better to have had no risk however reducing risk is quite important.)

   Timeline: Yearly.

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

   Procedure / Activity: Check the enterprise endpoint antivirus management console daily and resolve any virus/malware issues on endpoints within one business day.

   Measurement Tool: Enterprise endpoint antivirus management console reporting services.

   Timeline: Report yearly, monitor every business day.

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

   Procedure / Activity: Detect new vulnerabilities, identify and evaluate the risk, notify the appropriate support staff, confirm when vulnerability is resolved, accepted, or mitigated to an acceptable level.

   Measurement Tool: Quantity of issues identified and resolved.

   Timeline: Yearly.

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

   Procedure / Activity: Study for OSCP and pass test within three years. Study Python and bash shell scripting for OSCP certification. Maintain CPE's required for CISSP certification, pay annual dues for CISSP certification.

   Measurement Tool: Discuss OSCP certification progress with the CIO during routine department update meetings. CISSP certification validity can be verified online on-demand.

   Timeline: OSCP certification presented during or before 2020-2021 academic year. Providing OSCP certification will be proof that applicable programming skills were developed.