Subject	**Cybersecurity**
Strategic Plan Connection	**Institutional Efficiency:** **Goal Statement:** Strengthen systems, policies and procedures to create more proactive, responsive and effective internal processes. **Goal Intention:** While the College has changed dramatically over the last decade, the institution's operational infrastructure has not kept pace. COCC will examine and improve policies, procedures and systems to make them more efficient, effective and operationally sustainable to provide a high quality work and learning environment.
Prepared By	• Dan Cecchini, chief information officer • Wesley Dymond, information security administrator

INFORMATION SECURITY AT COCC

COCC created and filled the Information Security position within Information Technology Services (ITS) in 2011. ITS had identified the growing cybersecurity threats to the College and requested the position to focus on those new and growing risks.

Board of Directors Governance and Information Security

Cybersecurity is not just an IT-related activity; it is an enterprise-level activity that affects all parts of an organization. In the same way Boards have invested their time in fiscal governance for organizations, the storage and management of all organizational information assets in increasingly complex electronic systems adds a relatively new, but real risk parameter for Boards to be kept abreast of. It is important for Boards to know that College administration has controls in place to identify, prevent, mitigate and manage risk to the organization's business operations and the response to cybersecurity incidents. Boards can benefit from reports on: College cybersecurity activities and the risk associated with them, metrics on ITS cybersecurity performance, and efforts taken by the organization to monitor and mitigate risk.

Key points regarding information security governance:

- Cybersecurity is a College-wide risk management issue, not simply an IT issue. While ITS can mitigate many technology cybersecurity risks, many risks fall into the areas of business processes and personnel training.
- Awareness of legal and regulatory implications regarding information security risks as they relate to the college. The US Department of Education has made clear that Title IV schools must comply with cybersecurity regulations — including those found in the Gramm-Leach-Bliley Act (GLBA). At a minimum, Title IV schools must understand the requirements of GLBA and ensure compliance with those requirements. GLBA requires Title IV schools to take specific actions in order to protect personal information in their possession. One such action is that schools must develop their own cybersecurity programs. Where Title IV schools suffer cybersecurity breaches or are found to be deficient in cybersecurity protections, the Department of Education has made clear that such schools may face restrictions on Title IV funding, including a complete loss of eligibility.
- The College provides cyber security resources to the faculty, staff, and students in the following areas regarding Cybersecurity Risk:
    - Education
    - Protection
    - Remediation
- As a best practice, the College administration provide regular cybersecurity status updates for the Board.

TOP INFOSEC THREATS FACED BY COCC

PHISHING:

Cyber criminals routinely launch phishing campaigns against COCC. There are a variety of techniques used, from simple "iTunes card purchase" scams to active spear phishing (emulating COCC's president and/or members of the COCC Board of Directors.) These campaigns leverage myriad factors to increase the chances of success. The highest volume of phishing emails received occur during the start of terms and holidays. Adversaries actively monitor COCC and are aware of our term schedule, new board members and changes in presidents. The ITS department makes continual improvements in defensive measures and incident response strategies. On average, COCC's ITS department resolves phishing campaigns in less than four hours and with minimal impacts to College resources, employees, and community.

MALWARE & COMPUTER INFECTIONS:

Ransomware is arguably the most crippling cyber-crime affecting organizations today. Ransomware resolution typically includes shutting down an organization's technology for 1-3 weeks, thousands or tens of thousands of dollars for ransom, costs for forensics and cyber security consultation, and loss of trust in the organization. Virus technology has evolved since its inception it the 80's. Beyond ransomware, malware tactics employ numerous other techniques ranging from social engineering and stealth data exfiltration to using the compromised target as a gateway to other organizations. Leveraging tools used for legitimate College work, cyber-criminals attempt to attack our institution mostly through internet and email services.

MAKING A DIFFERENCE

COCC has developed a cybersecurity program and continues to review and update it as threats against our assets change and multiply.

INFORMATION SECURITY AWARENESS TRAINING

Information security awareness training has made a positive and powerful impact on COCC's cybersecurity defensive posture. After years of Information Security education and training by ITS, COCC's employees show an outstanding awareness of cyber-criminal tactics and an awareness of their part in defending the college from attacks. Information security professionals understand that employees are often the first line of defense. When new phishing campaigns launch against COCC, employees typically alert the ITS department within minutes. Employees have also displayed an impressive capability to detect internet malware tactics and reach out to COCC ITS for support and remediation.

PROTECTION

Intersecting technology and business processes for the purpose of safeguarding data, COCC ITS incorporates several defensive measures which have already proven to either defeat or mitigate threats. These processes and measures continually evolve at COCC to keep up with newly identified cybersecurity threats.

Disaster recovery testing with other departments college-wide shaped and improved our data recovery capabilities, reducing potentially disastrous outages to acceptable levels. We are currently developing an even more comprehensive and formal Disaster Recovery and Business Continuity Plan.

The goal for our Information Security program is to allow our ITS department to formulaically address cyber-security risks in a more holistic manner, and which continues to focus on identifying the threats, protecting the resources, and quickly and efficiently remediating attacks when they do get through our multi-layered cybersecurity defenses.