2013

CAMPUSWORKS INFORMATION TECHNOLOGY ASSESSMENT REVIEW AND TALON CYBER SECURITY AUDIT CROSSWALK

This document provides an executive summary of the CampusWorks Information Technology Assessment Review and Talon Cyber Audit of SCCCD's Information Technology as well as a crosswalk of the findings and District IT responses to those findings.

Dr. George Railey
Vice Chancellor of Educational Services and Institutional Effectiveness
10/10/2013

CAMPUSWORKS INFORMATION TECHNOLOGY ASSESSMENT REVIEW AND TALON CYBER SECURITY AUDIT CROSSWALK

In the fall of 2011 CampusWorks presented to the SCCCD Board its Information Technology Assessment First Look, Preliminary Report. This report provided an overall assessment of SCCCD's Information Technology and provided the executive team with preliminary findings and recommendations for IT strategy and Vision. CampusWorks reviewed requested documents, interviewed administration, faculty, and staff, compared data against CampusWorks and industry standards, identified gaps, and made recommendations.

Components of the CampusWorks assessment were administrative systems, academic technology, network and infrastructure, desktop computing, staffing, planning and decision-making. This assessment was broad in focus and provided an overarching view of SCCCD's Information Technology.

Subsequent to the presentation of the CampusWorks Information Technology Assessment Review presentation to the Board, Talon Cyber was asked to perform an audit, based on recommendations made by CampusWorks. The primary objective of this Cyber Security Audit was to assess the core elements of SCCCD's technology infrastructure to identify and evaluate technical weaknesses, deficiencies, and vulnerabilities impacting our information security posture, as well as technical controls and mechanisms related to informational security, so that recommendations could be defined to improve security and remediate security issues.

Talon cyber employed an electronic network systems analysis instrument to assess core elements of SCCCD's technology infrastructure to identify and evaluate technical weaknesses, deficiencies, and vulnerabilities impacting our information security.

In Talon Cyber's Audit Report Assessment Summary they found that:

> "SCCCD is doing well in the areas Talon Cyber evaluated. SCCCD's technical infrastructure is currently operating in a stable environment, functioning as intended and does not possess any critical or high-risk security vulnerabilities…" Some lower-risk security weaknesses were found, but they "…are not systemic in nature and do not severely jeopardize the confidentiality, integrity, or availability of (our) technical infrastructure or information assets through the presence of easily exploitable security vulnerabilities". As such, SCCCD has been shown to be demonstrating due diligence surrounding information security and their information security risk management program."

Talon Cyber produced their final "Cyber Security Audit Report" on June 17, 2012.

CAMPUSWORKS INFORMATION TECHNOLOGY ASSESSMENT REVIEW AND TALON CYBER SECURITY AUDIT CROSSWALK

CampusWorks	Findings	Cyber Security Audit (Talon Companies) Findings	Current Response Status
Administrative System	Magic form Process Analysis & proposed online alternative Need Seasoned Executive-level Chief Information Officer Reporting to the Chancellor	N/A N/A	Currently conducting Action Planning with executive survey presented to Chancellor's Cabinet on October 14, 2013.
Academic Technology	Low adoption of course management system (Blackboard) Disorganized and inconsistent delivery of services Need for instructional technology/classroom configuration issues to be addressed in a manner that conforms with the academic schedule and requirements	N/A N/A N/A N/A	Currently conducting Action Planning with executive survey presented to Chancellor's Cabinet on October 14, 2013.
Network Infrastructure	Unreliable wireless network Network Saturation at Reedley College Network vulnerable to intrusion multiple security issues	N/A N/A Unnecessary services running and associated ports present a target or opportunity for an attacker to focus on and attempt to compromise security	The systems cited in this finding fall into three categories, and are either: (1) outside our control, belonging to our Internet provider (CENIC)— "sealed" devices which we aren't allowed to change, or are (2) required to have the services

		weaknesses to bypass security controls and gain unauthorized accessLack of patches-Systems on network environment currently operating without the most current and up-to-date patches applied, including security fixes that mitigate software flaws and other security issues **Remedies:** 1. Reconfigure select systems to remove unnecessary services and close associated ports 2. enable firewalls on Windows Services to restrict remote accessibility and minimize exposure of services 3. Apply missing patches and establish patch management system	available, or have (3) already been remediated. Category (1): 198.189.22.1 belongs to CENIC; can't change. Category (2): 10.6.4.1 / 2 and 10.128.4.1 / 2 are our switches, and they require Telnet availability for remote diagnosis and configuration, so no action required. Category (3): 205.155.151.40 is the Fujitsu voice mail server, which has been remediated by disabling terminal services and fully applying applicable Windows patches. 10.96.4.135: this is a Cisco security camera recorder, and is a sealed device we aren't allowed to modify.205.155.151.40: this is the Fujitsu voice mail server, and all applicable patches were applied.10.160.32.57 (SWIAS04B): this is a server at WI, and the identified Apache "Mod_ssl" (actually "OpenSSL") vulnerability has been patched by RC technical staff using an updated version provided by the vendor.10.64.4.105 (SRCCLASS): this is a server at RC, and the identified Apache "Mod_ssl" (actually "OpenSSL") vulnerability has been patched by RC technical staff using an updated version provided by the vendor.10.136.4.1: this is a CTC switch, and SSH v1 has been disabled to remediate the vulnerability. 205.155.151.43: this is an old web server application supporting job applicant processing, which has been replaced by the new People Admin system. The new system is operational, so this application has been turned off. The old firewall has been replaced with a state of the art Palo Alto Networks

			firewall. The new firewall has been installed and is operational providing advanced security and intrusion protection. http://www.paloaltonetworks.com/products/overview/
Desktop Computing	N/A	N/A	
Staffing	Common IT Help Desk with common dispatch Tiered support model Staff professional development & cross-training Opportunities for advancement Purchased services	N/A N/A N/A N/A N/A	Currently conducting Action Planning with executive survey presented to Chancellor's Cabinet on October 14, 2013.
Planning	District in need of comprehensive technology tactical plan, inclusive of campus-based plans Data security plans Data breach response plans Disaster recovery and business Continuity plans (address federal, state and industry standards for data security) Technology Budget plan (over 3-5 years) Development of funded and transparent technology life cycle system needed Inadequate leveraging	N/A N/A N/A N/A (See Network Infrastructure Security above) N/A N/A N/A	Technology Committee is slated to begin this work as soon as constituent review is completed and committee is approved.

	of prior technology investments Lack of planning including project management, within technology area Disorganized and inconsistent delivery of services	N/A N/A	Currently conducting Action Planning with executive survey presented to Chancellor’s Cabinet on October 14, 2013.
Decision-Making	Significant Lack of Technology leadership and vision Challenges in governance, planning and project management	N/A N/A	Vice Chancellor of Educational Services leading districtwide technology planning.
Resources	Common systems leveraged across the district (establish districtwide hardware & software standards) Software license management Complete inventory of all technology inventory with aging analysis Address identity management & access	N/A (See Security Audit findings) N/A N/A	Currently conducting Action Planning with executive survey presented to Chancellor’s Cabinet on October 14, 2013.