# Security Review
# Conducted for
# State Center
# Community College District

Conducted by:
Bill Ouchark

**Review performed**
**November 12-15, 2013**

***Confidential Report***

CAMPUSWORKS

1767 Lakewood Ranch Blvd. #305
Bradenton FL 34211
T. 941.316.0308 | F. 941.954.2398

www.campusWorksinc.com

## Executive Overview

The following highlights District progress and opportunities for improvement in securing data, information and systems in the State Center Community College District. District IT staff used as the basis for their security task list findings of the 2011 CampusWorks Second Opinion Assessment and the Cyber Security Audit Report prepared by Talon Companies (6/27/2012).

This Security Review included investigation to ensure the items addressed had been thoroughly and successfully completed, as well as a review of current policies and procedures and a security scan of identified service systems at each of the campuses.

Highlights

- **GREAT PROGRESS ON INFRASTRUCTURE INVESTMENTS**
    - Network
    - Phone system
    - Firewall (protection from external threats)
    - Public Safety
- **GOOD PROGRESS IN BEST PRACTICE ADOPTION**
    - Server patching
    - Network layout & design
    - Server virtualization
- **POOR PROGRESS ON FUNDAMENTAL SECURITY-RELATED ISSUES**
    - Understanding & meeting compliance requirements (e.g. PCI, DMCA, HEOA)
    - Elimination of unencrypted communications
    - Community education on security practices
    - Account & password management
    - Adoption of practices to ensure key resources secured from internal threats
    - Security incident response
    - Tools adoption to assist in above
- **NO HEADWAY ON INFORMATION TECHNOLOGY GOVERNANCE**
    - Policy development & communication
    - Technology plan development & communication
    - Full understanding of IT roles & responsibilities in present day higher education environment

- **MISSED OPPORTUNITIES DUE TO ORGANIZATIONAL CHALLENGES**
    - Resource time saved by eliminating duplication of effort
    - Risk elimination by minimizing single points of failure
    - Improved disaster recovery & business continuity
    - Increased ROI by sharing resources (e.g. data centers, network monitoring software, common virtual servers)

## Summary of Observed Security Vulnerabilities & Issues of Potential Concern

1. **IT GOVERNANCE COMMITMENTS AND RESPONSIBILITIES**
    - IT leadership weak in ability to provide direction on critical components of present-day technology and security management within higher education including:
        - Alignment of technology efforts with strategic institutional goals
        - Relationship development supportive of executive leadership priorities
        - Alignment of business processes to best fit existing technology solutions

2. **INFORMATION SECURITY POLICIES, PROCEDURES & GUIDELINES**
    - Minimal evidence, beyond basic Acceptable Usage Agreement, of policy development at either District Office or campuses
    - Key policies that appear absent include:
        - Data Classification & Handling
        - Data Confidentiality Access and Security
        - Copyright Materials Handling
        - Mobile Device Security

3. **ENFORCEMENT**
    - The absence of important core policies that identify appropriate behavior in handling and protection of sensitive data and the consequences of improper or negligent conduct may hinder disciplinary action, as well as a represent potential liability to the institution in the event of compliance challenge or litigation

4. **TRAINING AND EDUCATION**
    - Limited or no training in support of security-related policy education or competency development among staff or faculty

5. **INFORMATION SECURITY PROGRAM**

- No available tools or services in place to assist staff in identifying detectable security vulnerabilities, or providing warning that procedures may need improvements. These tools can routinize efforts and leverage staff time.
- No accepted plan or goals specific to information security. (A draft plan from February 2007 was identified, but apparently has sat dormant.)
- No clearly identified or delineated responsibilities specific to information security, including organizational, compliance or incident response-related responsibilities
- Weak user password practices including:
    - Assignment of passwords to users that they cannot change
    - Assignment of initial passwords to users containing weak passwords including last name and date of birth for wireless access (and not allowing users to change them)
- No common centralized account/password administration domain (e.g. Active Directory)
- No self-service password change capability
- Minimal effort towards single or common sign-on
- Undefined or weak account retention policies and practices
- Undeveloped change procedures for privileged access as employees change roles or positions within the institution
- Poor procedure and communication in place between Human Resources and Information Technology departments for notification and action on account or privilege changes supporting employee change of employment (e.g. termination, change of position)
- Limited attention paid in addressing use of unencrypted or weak encryption technologies
    - Use of telnet for Ellucian Colleague
    - Use of pre-shared keys for wireless access (District Office)
    - Use of weak passwords for wireless access (FCC)
- Data Center risk mitigation and security recommendations include:
    - Introduction of fire suppression
    - Ensure each facility has environmental monitoring (temperature, humidity, flood) is functional and periodically tested
    - Improved stricter authorized entry controls (beyond basic key entry)
    - Improved video perimeter monitoring (including recorded entry)
- No documented technology security incident or management procedures

- No clearinghouse or process for reporting and tracking identified security concerns or issues (i.e. issues known to technical staff go unknown and untracked to leadership)
- Present Disaster Recovery and Business Continuity Planning should be reassessed
    - Proximity of backup sites for both District Office and FCC counter intuitive given availability and resources available at remote sites (e.g. Reedley)
    - Potential disaster scenarios should be assessed and present planning adjusted in response
        - Situation involving a train disaster on tracks between District Office and FCC may present high risk to present records backups
        - Possible paths across railway tracks present potential concerns
            - Currently fiber crosses at only one location, despite fact that new conduit has been installed at new underpass location
            - Distance between these two crossings still quite close together (estimate provided was <100 meters)
        - Situation involving long-term disruption to both power and natural gas service represents risk to generators at both District Office and FCC (natural gas is likely service to be cut in disaster situation)

6. **COMPLIANCE**

- Interviews suggest that the technology staff have a very limited understanding of technology-related compliance requirements
- Responses received specific to Payment Card Industry Data Security Standards (PCI DSS), including the absence of a written *Credit Card Security Policy*, suggest that the institution may not be PCI-compliant
- The absence in knowledge among the technology staff of who institutionally has been designated the Agent for Digital Millennium Copyright Act (DMCA), combined with the absence of a registered Agent to receive infringement claims with the U. S. Copyright Office, suggest that the institution may not be DMCA-compliant
- Similarly, the policy and student handbook information provided in response to the CampusWorks information request, as well as responses to interview questions, were inconclusive in establishing whether compliance requirements specific to policy or notification were met for either the FTC Red Flag Rules (RFR) or the Higher Education Opportunity Act (HEOA)
- Additional, information collected from technology staff indicated a prior history of potential data breach incidents, yet no understanding or familiarity was expressed of the California Data Breach Notification Law (SB 1386)

7. **NON-INTRUSIVE VULNERABILITY SCANNING**

- Scanning results of all identified key campus services (servers) identified that, in general, a best practice and methodological approach to patching server operating systems has been adopted
- Some issues, including those of a critical nature, were identified and complete reports including remediation recommendations were provided to campus technical staffs
- Of the issues identified, a minimal number were indicative of servers that might have been missed on certain patch applications, suggesting a review of procedures be undertaken to understand why this might have taken place and corrective action taken
- Additionally some of the findings were related to issues with unpatched network-facing applications, as opposed operating systems. This suggests patch procedure planning should be expanded to encompass these applications.
- The present Cisco video surveillance servers at all campuses were also identified as a point of concern. The issue with these systems may be more than simply a requirement to apply patches, as the generation of hardware deployed may be unable to support current software revisions. Given concerns expressed by staff with the overall satisfaction of these systems in general, this may be a good opportunity to undertake a wider review of the video surveillance infrastructure and identify options for direction.