

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
CHICO

Audit Report 08-19
November 7, 2008

Members, Committee on Audit

Melinda Guzman, Chair
Raymond W. Holdsworth, Vice Chair
Herbert L. Carter Kenneth Fong
Margaret Fortune George G. Gowgani
William Hauck

Staff

University Auditor: Larry Mandel
Senior Director: Michelle Schlack
IT Audit Manager: Greg Dove
Audit Manager: Gary Miller
Senior Auditor: Alec Lu

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction.....	3
Background	3
Purpose.....	4
Scope and Methodology	6

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance.....	8
Security Authority and Responsibility	8
Policy Issuance and Approval.....	8
Information Security Policy	9
Payment Card Industry Data Security Standard.....	10
Record Retention.....	10
Remote Computing	11
Employee Separation	12
Access Control	12
Decentralized Computing	13
Server Environments.....	13
Technical Vulnerabilities	13
Vulnerability Management	15
System Development and Change Management.....	16
Web Application Development and Maintenance	16
Web Application Vulnerabilities.....	17
Systems Security and Monitoring	18
Configuration Changes	18
Control of User Access	19
E-mail.....	20
Network Access	21
Password Standards.....	22
Network Monitoring	22
Granting of Privileged Access	23
Application Control.....	24
Firewalls and Routing and Switching Devices	25
Other Network Devices.....	26
Network Architecture.....	27
Review of Security Event Logs	27

CONTENTS

Protected Data..... 28
 Assessment and Inventory of Protected Information 28
 Threat Management 29
Lost/Stolen Computers..... 30

APPENDICES

APPENDIX A:	Personnel Contacted
APPENDIX B:	Campus Response
APPENDIX C:	Chancellor's Acceptance

ABBREVIATIONS

AD	Active Directory
CSU	California State University
CSUC	California State University, Chico
DMZ	Demilitarized Zone
DNS	Domain Name Service
EO	Executive Order
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITEC	Information Technology Executive Committee
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
PCI DSS	Payment Card Industry Data Security Standard
SNMP	Simple Network Management Protocol
Telnet	Telecommunication Network
WLAN	Wireless Local Area Network

EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor, the Board of Trustees, at its January 2008 meeting, directed that *Information Security* be reviewed. The Office of the University Auditor had not previously reviewed *Information Security* as a separate subject area audit.

We visited the California State University, Chico campus from June 23, 2008, through August 14, 2008, and audited the procedures in effect at that time.

Our study and evaluation identified issues that, if left unattended, would continuously impact the overall control environment. We identified a series of problems that were listed individually in this report; however, the underlying root cause of many of the problems identified was the overall organization of information technology (IT) services using a decentralized campus computing environment that was not consistently managed in the same professional manner as the services provided by the campus IT department. Also, the campus environment did not lend itself to timely creation and issuance of campus-wide IT policies.

In our opinion, the operational and administrative controls of information security in effect as of August 14, 2008, taken as a whole, were not sufficient to meet many of the objectives for a secured computing environment. While much of the campus IT department control environment was satisfactory and provided appropriate safeguards over the critical financial and student systems, the decentralized computing environments that were not under the purview of campus IT require significant improvement and management oversight.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

Our audit did not examine all aspects of information security, but was designed to assess the controls over management, increase awareness, and recommend implementation for significant security topics that are prevalent in the California State University (CSU) computing environment.

The following summary provides management with an overview of conditions requiring attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [] refer to page numbers in the report.

SECURITY GOVERNANCE [8]

The campus lacked an adequate process to ensure compliance with relevant laws, regulations, and general CSU policy related to information security. The process to review, approve, and disseminate information security policies, procedures, and guidelines was deficient. The campus information security plan had not been updated to address recent compliance requirements or the changing business organization. The campus and auxiliaries had not completed a Payment Card Industry Data Security Standard compliance summary plan to define their applicable vendor level and respective contractual requirements. The

campus had not completed a record retention action plan consisting of procedures to ensure appropriate and timely disposal of records/information. There were no controls in place for the management of remote machines connected to the internal campus network via virtual private network. Employees were not reminded of their ongoing legal responsibility for maintaining the security of protected data at the time of their separation. User accounts were being shared without proper accountability and approval.

DECENTRALIZED COMPUTING [13]

Administration of decentralized departmental server environments required improvement. Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. The campus lacked a standard process to manage vulnerabilities.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [16]

Change management procedures for web application and development required improvement. Web application vulnerabilities existed on one web application selected for testing.

SYSTEM SECURITY AND MONITORING [18]

The campus lacked policies and procedures that defined a formal periodic review of configuration changes for certain systems and devices. The administration of user accounts and the processes for requesting, approving, and monitoring user access to systems and applications were not adequately controlled. The administration of the e-mail system required improvement. The campus had not adequately secured the campus local area network. The campus password policy had not been enforced and extended to all departments and/or applications on campus. The campus lacked a formal process to identify and monitor all IT resources on the campus network. The process to manage users with privileged access required improvement. The campus had not assessed the need for administrative privileges on state purchased machines for the control of software applications. Firewalls and routing and switching devices were not always properly configured or adequately secured. The campus had not identified the security risks of hardware devices attached to the network. Internet accessible devices were located within the same segments as internal resources. The review of security event logs was not adequate.

PROTECTED DATA [28]

The campus had not conducted an overall security assessment of desktops with sensitive information. The campus did not actively monitor intrusion security events. The campus lacked a process to ensure that lost/stolen computers were properly investigated.

INTRODUCTION

BACKGROUND

State Administrative Manual Section 5300 states that information security means the protection of information and information systems, equipment, and people from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction. Pursuant to Government Code Section 11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, procedures, and filing requirements issued by the Office of Information Security and Privacy Protection, California Office of Information Security.

The California State University (CSU) *Information Security Policy*, dated August 2002, states that the Board of Trustees of the CSU is responsible for protecting the confidentiality of information in the custody of the CSU; the security of the equipment where this information is processed and maintained; and the related privacy rights of the CSU students, faculty, and staff concerning this information. It is also the collective responsibility of the CSU, its executives, and managers to ensure:

- ▶ The integrity of the data.
- ▶ The maintenance and currency of the applications.
- ▶ The preservation of the information in case of natural or manmade disasters.
- ▶ Compliance with federal and state regulations, including intellectual property and copyright.

It further states that campuses must have security policies and procedures that, at a minimum, implement information security, confidentiality practices consistent with these policies, and end-user responsibilities for the physical security of the equipment and the appropriate use of hardware, software, and network facilities. The policy applies to all data systems and equipment on campus that contain data deemed private or confidential and/or which contain mission critical data, including departmental, divisional, and other ancillary systems and equipment.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published an information security standard in 2005 as ISO/IEC 17799:2005 *Information Technology - Security Techniques - Code of Practice for Information Security Management*. This standard was subsequently renumbered as ISO/IEC 27002:2005 in July 2007 in order to bring it into line with the other ISO/IEC 27000-series standards, also known as the Information Security Management System (ISMS) Family of Standards. The ISMS Family of Standards comprises information security standards published jointly by the ISO and the IEC.

The CSU contracted with Unisys in 2006 to perform a series of on-site Information Security Assessment Reviews at nine campuses and the chancellor's office. This assessment was designed to perform a basic review of CSU information security as benchmarked against the industry-accepted standard, ISO 17799:2005, as well as all applicable state and federal laws.

The CSU also contracted with CH2MHill in 2007 for the development of comprehensive information security policies and standards. These policies and standards address the following areas: information security roles and responsibilities; risk management; acceptable use; personnel security; privacy; security awareness and training; third-party services security; IT security; configuration management and change control; access control; asset management; management of information systems; information security incident management; physical security; business continuity and disaster recovery; and legal and regulatory compliance. The Information Technology Advisory Committee, composed of the chief information officers from each campus, and the Information Security Advisory Committee, composed of the information security officers from each campus, was integrally involved in this policy development process in order to ensure that the final product was an appropriate fit for the CSU. This project began in September 2007 with the expectation that these policies and standards were to be completed by August 2008 for subsequent adoption and official systemwide distribution in late 2008. This timeline has now been extended an additional six months. Due to the pending status of this project during the time frame of the information security audits, these policies and standards were not used for evaluation of the campuses information security posture.

At California State University, Chico (CSUC), the office of information technology has overall responsibility for the management of campus systems and networks. However, a significant level of decentralization has shifted many critical IT responsibilities to ancillary departmental units throughout the campus.

PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration of information security and to determine the adequacy of controls over the related processes to evaluate adherence to an industry-accepted standard, ISO 17799/27002, *Code of Practice for Information Security Management*, and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the overall audit objective, specific goals included determining whether:

- ▶ Certain essential administrative and managerial internal controls are in place, including delegations of authority and responsibility, formation of oversight committees, executive-level reporting, and documented policies and procedures.
- ▶ A management framework is established to initiate and control the implementation of information security within the organization and management direction and support for information security is communicated in accordance with business requirements and relevant laws and regulations.
- ▶ All assets are accounted for and have a nominated owner/custodian who is granted responsibility for maintenance and control to achieve and maintain appropriate protection of organizational assets and information is appropriately classified to indicate the need, priorities, and expected degree of protection when handling the information.

- ▶ Security responsibilities are addressed prior to employment so that users are aware of information security threats and concerns, are equipped to support organizational security policy in the course of their normal work, and responsibilities are in place to ensure user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed.
- ▶ Responsibilities and procedures for the management of information processing and service delivery are defined and technical security controls are integrated within systems and networks.
- ▶ Access rights to networks, systems, applications, business processes, and data are controlled based on business and security requirements by means of user identification and authentication.
- ▶ Formal event reporting and escalation procedures are in place for information security events and weaknesses, and communication is accomplished in a consistent and effective manner allowing timely corrective action to be taken.
- ▶ The design, operation, use, and management of information systems are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.
- ▶ Web application development and change management processes and procedures are adequate to ensure that application security and accessibility is considered during the design phase, that testing includes protection against known vulnerabilities, and that the production servers are adequately protected.
- ▶ E-mail systems are properly configured and managed so that vulnerabilities are not allowed into the network, incidents are properly escalated, campus usage and retention guidelines are followed, and e-mail addresses are maintained in a central location to facilitate campus-wide communications.
- ▶ The operational security of selected operating systems is adequate to prevent the exploitation of vulnerabilities on the internal network by individuals who gain access to it from dial-in connections, the Internet, and hosts on the internal network.
- ▶ The Internet firewall system is sufficient to identify and thwart attacks from the external Internet and filter unwanted network traffic.
- ▶ Selected routing and switching devices are properly managed and configured to effectively provide the designated network security or traffic controls.
- ▶ Systems connected to the Internet make publicly available any information that may provide enticement to penetrate the Internet gateway.
- ▶ Web application vulnerabilities exist that provide the potential for an unauthorized party to subvert controls and gain access to critical and proprietary information, use resources inappropriately, interrupt business, or commit fraud.

SCOPE AND METHODOLOGY

The proposed scope of the audit, as presented in Attachment B, Audit Agenda Item 2 of the January 22-23, 2008, meeting of the Committee on Audit, stated that information security would include a review of the systems and managerial/technical measures for ongoing evaluation of data/information collected; identifying confidential, private, or sensitive information; authorizing access; securing information; detecting security breaches; and security incident reporting and response. Information security includes the activities/measures undertaken to protect the confidentiality, integrity, and access/availability of information including measures to limit collection of information, control access to data and assure that individuals with access to data do not utilize the data for unauthorized purposes, encrypt data in storage and transmission, and implement physical and logical security measures for all data repositories. Potential impacts include inappropriate disclosures of information; identity theft; adverse publicity; excessive costs; inability to achieve institutional objectives and goals; and increased exposure to enforcement actions by regulatory agencies.

In addition to the interviews and inquiry procedures affecting the operation and support of the network devices reviewed by the Office of the University Auditor, we also contracted with KPMG to perform a technical security assessment that included running diagnostic software designed to identify improper configuration of selected systems, servers, and network devices. The purpose of the technical security assessment was to determine the effectiveness of technology and security controls governing the confidentiality, integrity, and availability of selected campus assets. The assessment contained an internal component (within the campus network) and an external component (via the Internet) while encompassing a review of the security standards and processes that govern the CSUC campus. Specifically, this configuration testing included assessment of the following technologies:

- ▶ Selected operating system platforms.
- ▶ Border firewall settings.
- ▶ Selected routing and switching devices.
- ▶ Internet footprint analysis.
- ▶ Website vulnerability assessment.

Our study and evaluation were conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the internal administrative, compliance, and operational/technical controls over the management of information security. Specifically, we reviewed and tested:

- ▶ Information security policies and procedures.
- ▶ Information security organizational structure and management framework.
- ▶ Information asset management accountability and classification.

- ▶ Human resources security responsibilities.
- ▶ Administrative and technical security procedures, information processing, and service delivery.
- ▶ Access controls over networks, systems, applications, business processes, and data.
- ▶ Incident response, escalation, and reporting procedures.
- ▶ Compliance with relevant statutory, regulatory, and contractual security requirements.
- ▶ Web application security and applicable change management procedures.
- ▶ E-mail systems management and configuration.
- ▶ Operational security of selected operating system platforms.
- ▶ Security configurations of border firewall settings.
- ▶ Security configurations of selected routing and switching devices.
- ▶ Internet footprints of systems connected to the Internet.
- ▶ Website vulnerabilities stemming from exposures in the server's operating system, server administration practices, or flaws in the web application programming.

Our testing and methodology was designed to provide a managerial level review of key information security practices, which included detailed testing of a limited number of network and computing devices. Our review did not examine all aspects of information security, selected emerging technologies were excluded from the scope of the review, and our testing approach was designed to provide a view of the security technologies used to protect only key computing resources.

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

SECURITY GOVERNANCE

SECURITY AUTHORITY AND RESPONSIBILITY

The campus lacked an adequate process to ensure compliance with relevant laws, regulations, and general California State University (CSU) policy related to information security.

Although the campus had assigned roles for the information security officer, we found that the collaboration between this role and other roles on campus (i.e. legal, human resources) to support information security practices and ensure compliance with relevant laws, regulations, and contractual requirements was deficient.

The information security officer stated that the campus had not considered the collaboration between various departments to be necessary since the compliance function was typically addressed within the roles of each department.

A lack of collaboration between the information security officer and other oversight offices increases the risk that laws, regulations, and general CSU policy will not be enforced.

Recommendation 1

We recommend that the campus ensure compliance with relevant laws, regulations, and contractual requirements related to information security.

Campus Response

We concur. The campus will create a procedure by March 2009 to ensure compliance with relevant laws, regulations, and contractual requirements related to information security.

POLICY ISSUANCE AND APPROVAL

The process to review, approve, and disseminate information security policies, procedures, and guidelines was deficient.

We noted that:

- ▶ Best practices, procedures, and guidelines were issued by central information technology (IT); however, these practices were either not consistently followed, not sufficiently communicated to relevant users, or users felt that these practices were not applicable to their area.
- ▶ The information technology executive committee (ITEC) was specifically created to serve as the executive level forum for policy issuance, review, and dissemination; however, ITEC meetings had not been consistently held.

The chief information officer stated that ITEC meetings had not been held due to a vacant provost position and that this lack of a formal management forum resulted in the breakdown of communication between central IT and various departments on campus.

Failure to properly review, approve, and disseminate information security policies, procedures, and guidelines increases the risk that information security practices may not be consistent with campus standards and limits the effectiveness of information security governance.

Recommendation 2

We recommend that the campus improve its process to ensure that information security policies, procedures, and guidelines are properly disseminated through regular executive meetings, and implement measures to ensure compliance.

Campus Response

We concur. The campus will improve and document its process to ensure that information security policies, procedures, and guidelines are properly disseminated through regular executive meetings, and that measures are developed to ensure compliance by March 2009.

INFORMATION SECURITY POLICY

The campus information security plan had not been updated to address recent compliance requirements or the changing business organization.

The information security officer stated that the campus was waiting on the overall CSU information security policy for guidance before creating a campus-wide policy.

The lack of an information security policy increases the risk of misunderstandings regarding user responsibilities.

Recommendation 3

We recommend that the campus develop and document an information security plan taking into account its current business environment.

Campus Response

We concur. The campus will update the information security plan to address its current business environment by May 2009.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The campus and auxiliaries had not completed a Payment Card Industry Data Security Standard (PCI DSS) compliance summary plan to define their applicable vendor level and respective contractual requirements.

We found that:

- ▶ An annual risk assessment was not performed to determine comprehensive compliance obligations for credit card data maintained on servers and transmitted throughout the campus network as required by PCI DSS.
- ▶ Responsibility for assessing campus and auxiliary PCI DSS compliance was not defined.

The information security officer stated that there was a lack of coordination and communication between the campus and various departments to ensure compliance with PCI DSS requirements.

Failure to comply with PCI DSS requirements increases the risk of financial penalties and credit card usage restrictions, including termination of the campus' ability to accept credit cards.

Recommendation 4

We recommend that the campus:

- a. Conduct a PCI assessment to determine their applicable vendor level and respective PCI requirements.
- b. Define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

Campus Response

We concur. The campus will initiate a PCI assessment to determine our applicable vendor level and respective PCI requirements by April 2009. As part of this process, the campus will define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

RECORD RETENTION

The campus had not completed a record retention action plan consisting of procedures to ensure appropriate and timely disposal of records/information.

Executive Order (EO) 1031, *Systemwide Records/Information Retention and Disposition Schedules Implementation*, dated February 27, 2008, states that each campus must establish and publish procedures for the modification of retention and disposition schedules, as needed, to incorporate records unique to each campus; and annually review its records/information as listed on the schedules to determine if they should be destroyed or maintained.

The information security officer stated that the lack of coordination and communication between campus departments resulted in the failure to complete a record retention action plan.

Failure to complete a record retention plan increases the risk of inappropriate and untimely disposal of records/information.

Recommendation 5

We recommend that the campus complete a record retention action plan consisting of procedures to ensure appropriate and timely disposal of records/information in accordance with CSU record retention and disposition schedule time frames.

Campus Response

We concur. The campus will complete a record retention action plan outlining procedures to ensure appropriate and timely disposal of records/information in accordance with existing CSU record retention and disposition schedule time frames, and in compliance with the EO 1031 record retention policy by March 2009.

REMOTE COMPUTING

There were no controls in place for the management of remote machines connected to the internal campus network via a virtual private network.

The information security officer stated that security of non-university owned computers connecting to the campus network has always been the responsibility of the user. She further stated that, although the campus used technical controls to validate machines from known high-risk areas of the campus network, these controls had not been deployed to all machines due to the cost and complexity of these solutions.

The lack of security controls for remote users increases the risk that sensitive information could be inadequately secured and increases campus exposure to security breaches.

Recommendation 6

We recommend that the campus implement controls for the management of remote machines connected to the internal campus network via a virtual private network.

Campus Response

We concur. The campus will implement controls for the management of remote machines connected to the internal campus network via a virtual private network by April 2009.

EMPLOYEE SEPARATION

Employees were not reminded of their ongoing legal responsibility for maintaining the security of protected data at the time of their separation.

The information security officer stated that the campus was unaware that a security communication reminder should be included in their employee separation process.

Failure to notify separating employees of ongoing legal responsibility to maintain the security of protected data increases the risk of non-compliance with statutory information security requirements for any remaining access to, or unauthorized custody of, protected data that may be available to terminated employees.

Recommendation 7

We recommend that the campus modify their exit process to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data.

Campus Response

We concur. The campus already modified the exit process in November 2008 to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data.

ACCESS CONTROL

An acceptable use policy allowed for the sharing of user accounts in certain business instances; however, these exceptions were not properly documented or approved.

The information security officer stated that while the acceptable use policy allows for sharing of accounts, the intention of this exception was not clear and accounts may have been shared in cases, which were not justified.

Failure to properly document the use of shared accounts increases the risk that errors and misappropriations may go undetected.

Recommendation 8

We recommend that the campus reevaluate or clarify their acceptable use policy and, if appropriate, include procedures for documenting and approving exceptions.

Campus Response

We concur. The campus will create a procedure for documenting and approving sharing of account exceptions by March 2009.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Administration of decentralized departmental server environments required improvement.

We found that:

- ▶ Backups with confidential data were stored in an unencrypted format.
- ▶ Server hardening standards and log management guidelines were not consistently followed.

The information security officer stated that department system owners and server administrators were responsible for securing their systems and some server administrators had yet to comply with the campus server security procedures and guidelines.

Failure to properly administer decentralized servers increases the risk that servers may be compromised, resulting in loss of confidential data in the event of a security breach. Inadequate review of security logs increases the risk that malicious activity could go undetected or viruses or other malicious code could be embedded within the campus network and its resources, each of which could lead to confidential information being breached and not reported.

Recommendation 9

We recommend that the campus:

- a. Ensure that backups from decentralized servers with sensitive data are properly encrypted.
- b. Enforce the server hardening and log management practices for the decentralized servers.

Campus Response

We concur. The campus will create a policy to ensure that backups from decentralized servers containing Protected Level 1 information are properly encrypted, and that server hardening and log management practices for these decentralized servers are followed by May 2009.

TECHNICAL VULNERABILITIES

Technical vulnerabilities existed on a variety of decentralized systems throughout the campus.

Our external testing of selected servers disclosed the following vulnerabilities (for which specific details were provided to the campus):

Two servers were running older versions of Apache web server software which are susceptible to multiple vulnerabilities, two servers were running Simple Network Management Protocol (SNMP) which allowed the community names of these remote hosts to be guessed, two servers were vulnerable to File Transfer Protocol crash flaw, one remote Real Time Streaming Protocol server

suffers from multiple vulnerabilities, four servers were discovered with web application cross site scripting vulnerabilities, two servers were susceptible to Hypertext Transfer Protocol header overflow, three servers were running a vulnerable version of Hypertext Preprocessor with known security issues, three servers were vulnerable to the Apache web server chunk handling vulnerability, two servers were remote hosts running a version of Apache which was vulnerable to an off-by-one buffer overflow attack, one remote Telecommunication Network (Telnet) server was vulnerable to buffer overflow, one Bind Domain Name Service (DNS) server was vulnerable to buffer overflow attacks, one server was running software which allowed for IP discovery and layout, nine servers were running software which was vulnerable to authentication bypass, two servers were running legacy operating systems no longer supported by the vendor, one server was susceptible to directory traversal, two servers were running vulnerable versions of server authentication software (Secure Shell), six servers were running vulnerable versions of Virtual Network Computing, two servers were vulnerable to DNS zone transfers, one server was vulnerable to DNS cache poisoning, one server allowed remote connection using default credentials, one server was running a software version vulnerable to denial of service attacks, one server was vulnerable to Structured Query Language injection attacks, one server was running a service which allowed execution of arbitrary commands, one server was running rlogin services which may allow users to login and copy files between machines without typing passwords, two servers were running a vulnerable version of Remote Desktop Protocol, one server had guest account with excessive privileges.

Additionally, there was no process to ensure decentralized servers were not routinely patched, there was no baseline security standard for server security or application security, and professional application development standards and methodologies were absent or not adequate.

The information security officer stated that the lack of centralized IT oversight and direction had permitted the majority of these vulnerabilities to propagate in the decentralized computing environments not under the control of central IT.

Server vulnerabilities introduced by a lack of patching or inadequate development processes increase the risk of a remote attack on the server that could lead to server disablement, loss of protected confidential information, and the execution of malicious programs that could disable additional network resources.

Recommendation 10

We recommend that the campus repair all of the technical vulnerabilities that were identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.

- c. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application. This process would include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.
- d. Provide all the ancillary IT units with a security baseline standard for securing servers prior to allowing them to become Internet facing.

Campus Response

We concur. The campus will create a policy and standard that includes a campus-wide patch management process, create a security baseline standard to review applications for security vulnerabilities prior to deployment, and create an application development standard for new and existing code to which developers must comply prior to deploying any Internet-facing application. The standards will apply to both centralized and decentralized campus IT units and will be completed by March 2009. Additionally, the campus has already repaired many of the technical vulnerabilities that were identified and is actively working to mitigate the remainder by March 2009.

VULNERABILITY MANAGEMENT

The campus lacked a standard process to manage vulnerabilities.

We noted that:

- ▶ There was no formal process to ensure that vulnerabilities detected through individual department scans had been appropriately addressed and resolved. While documentation existed on the handling of various vulnerabilities, this process was decentralized and was not consistent across campus.
- ▶ Departments were not consistently performing periodic vulnerability scans.

The information security officer stated that department server administrators were responsible for performing their own scans and some server administrators had yet to comply.

Failure to address identified vulnerabilities may lead to a compromise in network resources and loss of protected confidential information.

Recommendation 11

We recommend that the campus develop a standard process to address identified vulnerabilities on all machines connected to the campus network and to ensure that all departments are performing periodic vulnerability scans.

Campus Response

We concur. The campus will create a standard process to address identified vulnerabilities on all machines connected to the campus network by March 2009. As of August 2008, the information security office is performing weekly vulnerability scans of all registered centralized and decentralized services.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

WEB APPLICATION DEVELOPMENT AND MAINTENANCE

Change management procedures for web application and development required improvement.

We noted the following deficiencies in our review of selected campus departments that perform web application and development:

- ▶ Formal approval was not required for projects put into production.
- ▶ Security criteria for testing procedures were not documented.
- ▶ User acceptance procedures were not documented.
- ▶ Programmers had unlimited access to source code.
- ▶ Developers had the ability to move applications into production.
- ▶ Production environment was not separated from the development environment.

In addition, we noted there was no standard process to ensure that web applications, which interface with campus systems, were reviewed and approved prior to moving into production.

The information security officer stated that department web application developers were responsible for the security of their web applications and consistent change management standards had not been developed or implemented.

The lack of proper change management procedures increases the risk that web application projects may be unauthorized, inconsistent with user expectations, and contain vulnerabilities.

Recommendation 12

We recommend that the campus:

- a. Develop a formal approval process for all web application development to ensure that they meet security standards established by the campus.
- b. Develop formal documentation of security criteria for testing procedures, including but not limited to, input and output validation tests.
- c. Develop formal documentation for user acceptance and deployment.

- d. Ensure that the web application source code is protected by limiting access to only those who need it.
- e. Limit developers' ability to move web applications into production and segregate production environment from development environment.

Campus Response

We concur. The campus will develop standards for campus web application development which will include testing procedures (including input and output validation tests), procedures for user acceptance and deployment, and procedures to ensure the web application source code is protected. The standard will also list controls required for migration of systems between development and production environments. The standards will be created by May 2009.

WEB APPLICATION VULNERABILITIES

Web application vulnerabilities existed on one web application selected for testing.

The web application allowed stack trace generation that displayed unnecessary information that was potentially useful to attackers and allowed the Autocomplete attribute for user credentials.

The information security officer stated that these vulnerabilities were the result of various causes, which includes programming oversight and the delay in upgrading patches and/or applications.

These exposures increase the risk that a remote attacker may be able to exploit vulnerabilities that could lead to loss of protected confidential information, and the execution of malicious programs on the server that could disable additional network resources.

Recommendation 13

We recommend that the campus repair the website vulnerabilities that were identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.

Campus Response

We concur. The campus will by May 2009, as per recommendation 10, create standards that include a campus-wide patch management process, and create a security baseline standard to review applications for security vulnerabilities prior to deployment. Additionally, the campus will create a standard to address the identification and mitigation of known vulnerabilities in new and existing web application code by May 2009.

SYSTEMS SECURITY AND MONITORING

CONFIGURATION CHANGES

The campus lacked policies and procedures that defined a formal periodic review of configuration changes for the following systems and devices:

- ▶ Firewalls.
- ▶ Switches.
- ▶ Routers.
- ▶ Operating systems.

The periodic review of these assets was occurring informally as part of network operational responsibilities; however, this informal process was not adequate to ensure that these network devices adhere to the latest configuration standards and updates.

The information security officer stated that the campus had not considered it a necessity to formally document all of its network processes.

Lack of periodic review of system and device configuration increases the risk of having inconsistent and deprecated standards, which may permit malicious activity to go undetected.

Recommendation 14

We recommend that the campus:

- a. Develop policies and procedures and establish a formal process for the review of system configurations that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.
- b. Implement a formal sign-off process by appropriate campus personnel to help establish an audit trail of these reviews.

Campus Response

We concur. The campus will develop a standard and procedures for the review of system configurations that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices, and implement a formal sign-off process by appropriate campus personnel to help establish an audit trail of these reviews by March 2009.

CONTROL OF USER ACCESS

The administration of user accounts and the processes for requesting, approving, and monitoring user access to systems and applications were not adequately controlled.

Our review of user accounts disclosed the following:

- ▶ User accounts were active even though the employees had been terminated.
- ▶ Several accounts lacked confidentiality agreements on file.
- ▶ Periodic management review of user access within all systems and applications containing protected data was not performed and documented.

The information security officer stated that system owners/managers were responsible for provisioning/de-provisioning user access and performing periodic user access reviews and that the lack of a central user access process and system contributed to these deficiencies.

Failure to properly administer user accounts increases the risk of inappropriate access.

Recommendation 15

We recommend that the campus:

- a. Formalize a process for managing and removing user accounts.
- b. Ensure that confidentiality agreements are completed and retained for those users with access to protected data.
- c. Conduct and document regular reviews of user access to systems containing protected data.

Campus Response

We concur. The campus will create a process for managing and removing user accounts, ensure that confidentiality agreements are completed and retained for those users with access to Protected Level 1 information, and conduct and document regular reviews of user access to systems containing Protected Level 1 information by April 2009.

E-MAIL

The administration of the e-mail system required improvement.

We noted that:

- ▶ Certain e-mail systems could also double as a file server and/or class development tool.
- ▶ Encryption had not been utilized for authentication to e-mail systems.
- ▶ E-mail systems had open ports, which may not be required to provide e-mail service.

The information security officer stated that several of the deficiencies were related to unauthorized e-mail servers managed outside of central IT and that other deficiencies were not addressed because of the end-user impact of these controls.

Inadequate security of e-mail systems increases the risk of campus susceptibility to network vulnerabilities and increases the risk of inappropriate access to protected data.

Recommendation 16

We recommend that the campus:

- a. Evaluate the e-mail requirements and determine whether file servers included on servers with e-mail systems creates unwarranted security risks.
- b. Implement encryption for the authentication to e-mail systems.
- c. Evaluate the ports necessary for e-mail service and disable other ports not needed to provide such service.

Campus Response

We concur. The campus will perform an assessment to determine the level of acceptable risk when file servers are included on servers with e-mail systems and evaluate the ports necessary only for e-mail service by May 2009. Currently, all new campus computers are deployed requiring encrypted authentication to e-mail systems. By May 2009, e-mail clients connecting to the campus e-mail server will be required to use encrypted-only authentication and there will be a documented process for exceptions.

NETWORK ACCESS

The campus had not adequately secured the campus local area network (LAN).

We found that:

- ▶ There were no restrictions on machine access to the campus LAN. The campus permitted automatic wired access via any operable Ethernet jack to all machines without requiring registration or confirmation of adequate security updates. Also, user authentication was not required to verify the identity of the user so unauthorized users could easily access normally protected areas of the campus internal network.
- ▶ Wireless local area network (WLAN) was unencrypted. WLAN users were required to authenticate to the WLAN; however, wireless traffic was not encrypted.

The information security officer stated that although the campus was aware of the issue regarding authentication to the wired network, a mitigating technology had yet to be implemented. She further stated that the Aruba wireless solution, being implemented currently, would provide encryption of the wireless network.

Inadequate control over access to the campus network increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

Recommendation 17

We recommend that the campus:

- a. Strengthen controls to adequately secure the campus LAN.
- b. Implement a log-on banner to remind users of the acceptable use policy and risks of using wireless networks.
- c. Segregate the WLAN accessible to the public from all internal network resources.
- d. Consider WLAN session time-outs to mitigate the risks of attacks through an open network.

Campus Response

We concur. The campus will strengthen controls to secure the campus LAN by May 2009. A log-on banner to remind users of the acceptable use policy and risks of using wireless networks was implemented in August 2008. However, at the time of the audit, our publicly accessible WLAN was already segregated from all internal network resources and included a session time-out to mitigate the risks of attacks through an open network.

PASSWORD STANDARDS

The campus password policy had not been enforced and extended to all departments and/or applications on campus.

We noted the following:

- ▶ Some departments with sensitive applications that require user login did not consistently apply the campus password policy.
- ▶ The central server team had an informal process for assigning passwords to administrative and service accounts.

The information security officer stated that while most campus applications authenticate to Lightweight Directory Access Protocol (LDAP) or Active Directory (AD), they have not inventoried applications with stand-alone authentication to target them for conversion to LDAP/AD authentication or to ensure they are following campus password policy. She further stated that failure of the server team to conform to password standards was due to the limited number of people with administrative and service accounts.

The lack of standard password policies for critical applications and for accounts with administrative privileges increases the risk for both easily guessed passwords and possible unauthorized access to network resources and confidential information.

Recommendation 18

We recommend that the campus ensure that authentication to sensitive applications and accounts with privileged access conform to the campus password policy.

Campus Response

We concur. The campus will adopt the CSU password policy and create a process to ensure that authentication to sensitive applications and accounts with privileged access conform to the password policy by March 2009.

NETWORK MONITORING

The campus lacked a formal process to identify and monitor all IT resources on the campus network, whether owned and managed by central IT or by ancillary IT groups.

We noted that any user on the network had the ability to place a server on the campus network without central IT permission.

The information security officer stated that although there were process controls in place, there were no physical/technical controls to stop the proliferation of servers on campus. Further, she stated that there was no policy restricting users from setting up individual servers.

The inability to identify and monitor all campus IT resources (servers, workstations, and laptops) increases the risk that the campus will be vulnerable to both internal and external attacks that could slow or bring down the network. This also increases the risk that an attacker could inject malicious code or viruses into the network or compromise confidential information.

Recommendation 19

We recommend that the campus:

- a. Restrict the ability to add servers to the campus network and implement a formal process for campus users to request such network service.
- b. Identify all current IT assets (including hardware, software, operating system versions, etc.) on the campus network and implement a process to monitor for adequate security.

Campus Response

We concur. The campus will, by March 2009, create a process to ensure that all current IT assets on the campus network are monitored for security in accordance with the security baseline standard, and that a process exists to evaluate additional assets before they are placed on the campus network.

GRANTING OF PRIVILEGED ACCESS

The process to manage users with privileged access required improvement.

We noted:

- ▶ There was no complete inventory of users with privileged accounts.
- ▶ Exceptions to extended user access after an employee had been terminated were not properly documented. We noted several accounts that were extended without clarification or purpose.
- ▶ There was no formal documentation and/or approval for the granting of administrative and service accounts, and as a result, logging and tracking had not been performed.

The information security officer stated that the provisioning and de-provisioning of privileged user access is not centrally managed. She also stated that the lack of a formal process for the granting of privileged access resulted in the limited documented controls (i.e. logging and tracking).

The lack of a standard process to grant and remove privileges may lead to inadequate segregation of duties, the granting of accounts not based on the principle of least privilege, and/or unauthorized access.

Recommendation 20

We recommend that the campus:

- a. Establish a formal standard for the granting of privileged accounts taking into account the criteria for individuals who should have access, roles, and responsibilities for these resources; and develop a method to track, review, and periodically audit this type of access.
- b. Develop a process to ensure that all privileged access is removed when an employee terminates and document all exceptions to this process.

Campus Response

We concur. The campus will, by March 2009, create a standard to track and document the use of privileged access on campus, and will develop a process to ensure that all privileged access is removed when an employee terminates and document all exceptions to this process.

APPLICATION CONTROL

The campus had not assessed the need for administrative privileges on state purchased machines for the control of software applications.

The information security officer stated that certain users may need administrative privileges on their computers and that an overall assessment had not been performed to determine the administrative access privileges required for certain tasks.

Local administrative accounts in which users have the ability to install their own applications increases the risk that applications may violate CSU policy and/or expose the campus network to other vulnerabilities.

Recommendation 21

We recommend that the campus perform an assessment of business need for local administrative accounts and disable unnecessary privileges to restrict the use of unauthorized software.

Campus Response

We concur. The campus will, by April 2009, perform an assessment of business need for local administrative accounts and disable unnecessary privileges to restrict the use of unauthorized software.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

Firewalls and routing and switching devices were not always properly configured or adequately secured.

Our review of the border firewall and routing and switching devices disclosed that:

- ▶ Four devices and the border firewall were configured with SNMP version 1, which was unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ Three devices were enabled with Telnet, which could allow a remote attacker to obtain confidential authentication tokens allowing remote access to the devices since the user logins, passwords, and commands are transferred across the network in clear text.
- ▶ One device was configured with Secure Shell Protocol version 1, which could allow an attacker to perform a man-in-the-middle attack and capture network traffic and possibly authentication credentials.
- ▶ Two devices were running Open Shortest Path First with clear text authentication, which could allow an attacker to capture network traffic, perform a network wide denial of service or a man-in-the-middle attack.

The information security officer stated that these vulnerabilities were due to staff oversight or the lack of resources to implement the required technology.

These exposures increase the risk that a remote attacker may be able to gain access to network resources and exploit vulnerabilities that could lead to the loss of protected confidential information and the execution of malicious programs on the server that could potentially disable additional network resources.

Recommendation 22

We recommend that the campus repair all of the network device vulnerabilities that were identified and presented in detail to the campus.

In addition, we recommend that the campus formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.

Campus Response

We concur. The campus repaired or remediated all of the network device vulnerabilities that were identified and presented to the campus by August 2008. The campus will, by April 2009, create a documented security baseline standard that requires the review of network devices for security

vulnerabilities prior to deployment, and mitigate network device vulnerabilities that were identified and presented in detail to the campus.

OTHER NETWORK DEVICES

The campus had not identified the security risks of hardware devices attached to the network.

We noted the following:

- ▶ The security posture of modems was unknown. We noted 7 of 34 analog lines were identified as having modems connected. However, the security posture of these modem connections was unknown.
- ▶ The campus had not documented a periodic assessment of rogue wireless access points including disposition of exceptions.
- ▶ Printers were accessible via a web interface within the LAN and set up with default user ID and password.

The information security officer stated that the review of modem security and the failure to document periodic assessments of rogue wireless access points was an oversight. She also stated that the campus was aware of the issues regarding security of printers; however, due to the significant variety of campus printers, they were unable to address all associated vulnerabilities or implement a standard technical control.

Inadequate control over hardware devices increases the risk of loss, inappropriate use of state resources, and exposure to information security breaches.

Recommendation 23

We recommend that campus:

- a. Assess the security posture of identified modems to ensure the modems are properly secured.
- b. Document the periodic assessment of unauthorized wireless access points.
- c. Perform and document an assessment of risks related to the accessibility of printers via web interface.

Campus Response

We concur. The campus will, by March 2009:

- a. Assess the security posture of identified modems to ensure the modems are properly secured.
- b. Document the periodic assessment of unauthorized wireless access points.

- c. Perform and document an assessment of risks related to the accessibility of printers via web interface.

NETWORK ARCHITECTURE

Internet accessible devices were located within the same segments as internal resources. Normally, these Internet accessible devices were segmented into a demilitarized zone (DMZ) such that if these devices were compromised, there was separation among other internal network resources.

The information security officer stated that the campus had considered more segmentation within the campus network architecture, including the implementation of a DMZ, but lacked the resources to implement the required technologies.

Inadequate segmentation of publicly accessible devices from internal resources increases the risk that compromised devices could be used to pivot to other network targets and launch attacks against internal resources if a layered security model is not used.

Recommendation 24

We recommend that the campus review its current network topology and determine if Internet accessible devices should be logically separated from devices residing within the internal network.

Campus Response

We concur. The campus will, by April 2009, review its current network topology and determine if Internet accessible devices should be logically separated from devices residing within the internal network.

REVIEW OF SECURITY EVENT LOGS

The review of security event logs was not adequate.

We found that:

- ▶ The server team had enabled the logging of security events for Windows and UNIX servers. However, there was no periodic review of these logs and they were only stored for 16 hours due to memory and storage limitations.
- ▶ The network team informally reviewed security logs, reports, and e-mails that were received from configuration management tools that monitor devices. However, there was no formal process or procedure in place to review these logs.

The information security officer stated that resource constraints had limited the amount of time that personnel could spend manually reviewing logs.

Inadequate retention and review of security logs increases the risk that malicious activity could go undetected or viruses or other malicious code could be embedded within the campus network and its resources, each of which could lead to confidential information being breached and not reported.

Recommendation 25

We recommend that the campus:

- a. Establish a formal process to regularly review and analyze the security logging data to assist in identifying potential network vulnerabilities and breaches on campus systems. This process could include the use of tools and analytical methods, defining personnel responsibilities, reviewing frequency, and reporting/escalating processes.
- b. At a minimum, copy the critical logs to an ancillary server so that they can be retained for an appropriate time frame and be available for subsequent review if needed.

Campus Response

We concur. The campus will create a policy and procedures to regularly review and analyze security logging data to assist in identifying potential network vulnerabilities and breaches on campus systems by March 2009. These policies and procedures will include the use of tools and analytical methods, defining personnel responsibilities, reviewing frequency, and reporting/escalating processes. The policy and procedures will include copying critical logs to an ancillary server so that they can be retained for an appropriate time frame and be available for subsequent review if needed.

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

The campus had not conducted an overall security assessment of desktops with sensitive information.

While the campus had conducted an overall assessment of servers on the network with sensitive information, this process was not performed for the desktops on campus. In addition, the current data classification policy did not provide guidance on the storage and transmission of sensitive information kept on other forms of media (i.e., removable media, electronic communications, etc.).

The information security officer stated that the assessment of confidential data on servers was conducted and it was their intention to perform a similar assessment of desktops. She further stated that the campus had been waiting on the overall CSU information security standards for guidance before modifying the campus data classification standard.

Inadequate accountability of personal confidential information or to protected information increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

Recommendation 26

We recommend that the campus:

- a. Conduct an assessment of all campus computers to ensure security of protected information.
- b. Revise the current data classification policy to provide guidance on the storage and transmission of sensitive information.

Campus Response

We concur. The campus will revise the current data classification policy to provide guidance on the storage and transmission of Protected Level 1 information and conduct a survey of campus desktop users to identify and secure systems with Protected Level 1 information by March 2009.

THREAT MANAGEMENT

The campus did not actively monitor intrusion security events. Furthermore, the network devices were not configured with any automated rules to respond to network security events in order to restrict or block traffic from potential security threats.

The information security officer stated that server based intrusion detection had been piloted but not implemented campus-wide, while network intrusion detection was assumed to be delivered as a part of infrastructure terminal resources project.

Inadequate procedures for the monitoring of and response to security incidents increase the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

Recommendation 27

We recommend the campus implement an intrusion detection system to monitor and respond to potential security threats.

Campus Response

We concur. The campus will implement a host (desktop and server) based intrusion detection system to monitor and respond to potential security threats by March 2009. The campus will also develop a plan for implementation of the Juniper network based intrusion detection system by March 2009.

LOST/STOLEN COMPUTERS

The campus lacked a process to ensure that lost/stolen computers were properly investigated by the information security office to determine the disposition of sensitive information on computers and/or whether further action was required.

The information security officer stated that while university police and the information security office often worked together in the investigation of desktop or server security incidents, the lack of procedures to notify the information security office of stolen computers was an oversight.

Inadequate procedures for the investigation of protected data increases the risk that information security breaches could go unreported resulting in significant financial penalty and damage to the campus' reputation.

Recommendation 28

We recommend that the campus develop and implement a computer loss-theft checklist to ensure that the investigation and certification of possible protected data on lost/stolen computers is sufficiently documented and retained.

Campus Response

We concur. The campus will develop and implement a computer loss-theft checklist to ensure that the investigation and certification of possible protected data on lost or stolen computers is sufficiently documented and retained by December 2008.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Paul J. Zingg	President
Tom Alden	Analyst/Programmer, Regional and Continuing Education
Miles Allen	Director, Business and Finance Technology
Brooke Banks	Information Security Officer
Andi Beach	Director, Payroll, Benefits, Human Resources Information Systems
Pat Berry	Web Application Development Coordinator
Elbert Chan	Network Analyst, College of Engineering
Scott Claverie	Director, Communication Services
Jim Cragle	Analyst/Programmer, Financial Aid and Scholarship Office
Gene Edinger	Network Analyst, College of Business
Beverly Gentry	Director of Strategic Planning, Business and Finance
Robyn Hafer	Director of Advancement Services, University Development and Advancement
Lorraine Hoffman	Vice President, Business and Finance
Jean Irving	University Registrar, Student Records and Registration
Deborah Kuechel	Program Manager, Data Warehouse
Debbie McElroberts	Director, Application Development
Andrea Mox	Manager, User Services
Jason Musselman	Technical Security Analyst
Matt Norby	Director, Associated Students Information Technology
Bill Post	Vice Provost, Information Resources/Chief Information Officer
Linda Post	Associated Director, Enterprise Technical Planning and Support
Dan Reed	Interim Director, Financial Aid and Scholarship
Jerry Ringel	Director, Computing and User Support
Tom Rosenow	Director of Application Development and Tech Support, Enrollment Management
Phyllis Weddington	Director, Enterprise Technical Planning and Support
Doug Wilson	Technical Analyst, Payroll, Benefits, Human Resources Information Systems

California State University, Chico
Chico, California 95929-0025

Office of the Vice President for Business and Finance
Office: 530-898-6231 Fax: 530-898-4513



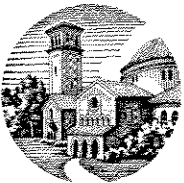
December 11, 2008

RECEIVED
UNIVERSITY AUDITOR

DEC 15 2008

THE CALIFORNIA STATE
UNIVERSITY

Mr. Larry Mandel
University Auditor
The California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4210



Dear Mr. Mandel:

Enclosed is California State University, Chico's response to the CSU Information Security Audit Report 08-19. We appreciate the time and effort your office has invested in the review of our procedures and internal controls. We welcome the report's recommendations and will take the actions necessary to address them.

If you have any questions or require additional information, please do not hesitate to contact me.

Sincerely,

Lorraine B. Hoffman
Vice President for Business and Finance

cc: Paul J. Zingg
Sandra Flake
Bill Post
Brooke Banks

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
CHICO

Audit Report 08-19

SECURITY GOVERNANCE

SECURITY AUTHORITY AND RESPONSIBILITY

Recommendation 1

We recommend that the campus ensure compliance with relevant laws, regulations, and contractual requirements related to information security.

Campus Response

We concur.

The campus will create a procedure by March 2009 to ensure compliance with relevant laws, regulations, and contractual requirements related to information security.

POLICY ISSUANCE AND APPROVAL

Recommendation 2

We recommend that the campus improve its process to ensure that information security policies, procedures, and guidelines are properly disseminated through regular executive meetings, and implement measures to ensure compliance.

Campus Response

We concur.

The campus will improve and document its process to ensure that information security policies, procedures, and guidelines are properly disseminated through regular executive meetings, and that measures are developed to ensure compliance by March 2009.

INFORMATION SECURITY POLICY

Recommendation 3

We recommend that the campus develop and document an information security plan taking into account its current business environment.

Campus Response

We concur.

The campus will update the information security plan to address its current business environment by May 2009.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Recommendation 4

We recommend that the campus:

- a. Conduct a PCI assessment to determine their applicable vendor level and respective PCI requirements.
- b. Define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

Campus Response

We concur.

The campus will initiate a PCI assessment to determine our applicable vendor level and respective PCI requirements by April 2009. As part of this process, the campus will define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

RECORD RETENTION

Recommendation 5

We recommend that the campus complete a record retention action plan consisting of procedures to ensure appropriate and timely disposal of records/information in accordance with CSU record retention and disposition schedule time frames.

Campus Response

We concur.

The campus will complete a record retention action plan outlining procedures to ensure appropriate and timely disposal of records/information in accordance with existing CSU record retention and disposition schedule time frames, and in compliance with Executive Order 1031 record retention policy by March 2009.

REMOTE COMPUTING

Recommendation 6

We recommend that the campus implement controls for the management of remote machines connected to the internal campus network via a virtual private network.

Campus Response

We concur.

The campus will implement controls for the management of remote machines connected to the internal campus network via a virtual private network by April 2009.

EMPLOYEE SEPARATION

Recommendation 7

We recommend that the campus modify their exit process to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data.

Campus Response

We concur.

The campus already modified the exit process in November 2008 to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data.

ACCESS CONTROL

Recommendation 8

We recommend that the campus reevaluate or clarify their acceptable use policy and, if appropriate, include procedures for documenting and approving exceptions.

Campus Response

We concur.

The campus will create a procedure for documenting and approving sharing of account exceptions by March 2009.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Recommendation 9

We recommend that the campus:

- a. Ensure that backups from decentralized servers with sensitive data are properly encrypted.
- b. Enforce the server hardening and log management practices for the decentralized servers.

Campus Response

We concur.

The campus will create a policy to ensure that backups from decentralized servers containing Protected Level 1 information are properly encrypted, and that server hardening and log management practices for these decentralized servers are followed by May 2009.

TECHNICAL VULNERABILITIES**Recommendation 10**

We recommend that the campus repair all of the technical vulnerabilities that were identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.
- c. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application. This process would include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.
- d. Provide all the ancillary IT units with a security baseline standard for securing servers prior to allowing them to become Internet facing.

Campus Response

We concur.

The campus will create a policy and standard that includes a campus-wide patch management process, create a security baseline standard to review applications for security vulnerabilities prior to deployment, and create an application development standard for new and existing code to which developers must comply prior to deploying any Internet-facing application. The standards will apply to both centralized and decentralized campus IT units, and will be completed by March 2009.

Additionally, the campus has already repaired many of the technical vulnerabilities that were identified, and is actively working to mitigate the remainder by March 2009.

VULNERABILITY MANAGEMENT**Recommendation 11**

We recommend that the campus develop a standard process to address identified vulnerabilities on all machines connected to the campus network and to ensure that all departments are performing periodic vulnerability scans.

Campus Response

We concur.

The campus will create a standard process to address identified vulnerabilities on all machines connected to the campus network by March 2009. As of August 2008, the Information Security Office is performing weekly vulnerability scans of all registered centralized and decentralized services.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

WEB APPLICATION DEVELOPMENT AND MAINTENANCE

Recommendation 12

We recommend that the campus:

- a. Develop a formal approval process for all web application development to ensure that they meet security standards established by the campus.
- b. Develop formal documentation of security criteria for testing procedures, including but not limited to, input and output validation tests.
- c. Develop formal documentation for user acceptance and deployment.
- d. Ensure that the web application source code is protected by limiting access to only those who need it.
- e. Limit developers' ability to move web applications into production and segregate production environment from development environment.

Campus Response

We concur.

The campus will develop standards for campus web application development which will include testing procedures (including input and output validation tests), procedures for user acceptance and deployment, and procedures to ensure web application source code is protected. The standard will also list controls required for migration of systems between development and production environments. The standards will be created by May 2009.

WEB APPLICATION VULNERABILITIES

Recommendation 13

We recommend that the campus repair the website vulnerabilities that were identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.

Campus Response

We concur.

The campus will by May 2009, as per Recommendation #10, create standards that include a campus-wide patch management process, and create a security baseline standard to review applications for security vulnerabilities prior to deployment. Additionally, the campus will create a standard to address the identification and mitigation of known vulnerabilities in new and existing web application code by May 2009.

SYSTEMS SECURITY AND MONITORING

CONFIGURATION CHANGES

Recommendation 14

We recommend that the campus:

- a. Develop policies and procedures and establish a formal process for the review of system configurations that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.
- b. Implement a formal sign-off process by appropriate campus personnel to help establish an audit trail of these reviews.

Campus Response

We concur.

The campus will develop a standard and procedures for the review of system configurations that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices, and implement a formal sign-off process by appropriate campus personnel to help establish an audit trail of these reviews by March 2009.

CONTROL OF USER ACCESS

Recommendation 15

We recommend that the campus:

- a. Formalize a process for managing and removing user accounts.
- b. Ensure that confidentiality agreements are completed and retained for those users with access to protected data.
- c. Conduct and document regular reviews of user access to systems containing protected data.

Campus Response

We concur.

The campus will create a process for managing and removing user accounts, ensuring that confidentiality agreements are completed and retained for those users with access to Protected Level 1 information, and conducting and documenting regular reviews of user access to systems containing Protected Level 1 information by April 2009.

E-MAIL

Recommendation 16

We recommend that the campus:

- a. Evaluate the e-mail requirements and determine whether file servers included on servers with e-mail systems creates unwarranted security risks.
- b. Implement encryption for the authentication to e-mail systems.
- c. Evaluate the ports necessary for e-mail service and disable other ports not needed to provide such service.

Campus Response

We concur.

The campus will perform an assessment to determine the level of acceptable risk when file servers are included on servers with e-mail systems and evaluate the ports necessary only for e-mail service by May 2009. Currently, all new campus computers are deployed requiring encrypted authentication to e-mail systems. By May 2009, e-mail clients connecting to the campus e-mail server will be required to use encrypted-only authentication and there will be a documented process for exceptions.

NETWORK ACCESS

Recommendation 17

We recommend that the campus:

- a. Strengthen controls to adequately secure the campus LAN.
- b. Implement a log-on banner to remind users of the acceptable use policy and risks of using wireless networks.
- c. Segregate the WLAN accessible to the public from all internal network resources.
- d. Consider WLAN session time-outs to mitigate the risks of attacks through an open network.

Campus Response

We concur.

The campus will strengthen controls to secure the campus LAN by May 2009. A log-on banner to remind users of the acceptable use policy and risks of using wireless networks was implemented in August 2008.

However, at the time of the audit, our publicly accessible WLAN was already segregated from all internal network resources and included a session time-out to mitigate the risks of attacks through an open network.

PASSWORD STANDARDS

Recommendation 18

We recommend that the campus ensure that authentication to sensitive applications and accounts with privileged access conform to the campus password policy.

Campus Response

We concur.

The campus will adopt the CSU password policy and create a process to ensure that authentication to sensitive applications and accounts with privileged access conform to the password policy by March 2009.

NETWORK MONITORING

Recommendation 19

We recommend that the campus:

- a. Restrict the ability to add servers to the campus network and implement a formal process for campus users to request such network service.

- b. Identify all current IT assets (including hardware, software, operating system versions, etc.) on the campus network and implement a process to monitor for adequate security.

Campus Response

We concur.

The campus will, by March 2009, create a process to ensure that all current IT assets on the campus network are monitored for security in accordance with the security baseline standard, and that a process exists to evaluate additional assets before they are placed on the campus network.

GRANTING OF PRIVILEGED ACCESS

Recommendation 20

We recommend that the campus:

- a. Establish a formal standard for the granting of privileged accounts taking into account the criteria for individuals who should have access, roles, and responsibilities for these resources; and develop a method to track, review, and periodically audit this type of access.
- b. Develop a process to ensure that all privileged access is removed when an employee terminates and document all exceptions to this process.

Campus Response

We concur.

The campus will, by March 2009, create a standard to track and document the use of privileged access on campus, and will develop a process to ensure that all privileged access is removed when an employee terminates and document all exceptions to this process.

APPLICATION CONTROL

Recommendation 21

We recommend that the campus perform an assessment of business need for local administrative accounts and disable unnecessary privileges to restrict the use of unauthorized software.

Campus Response

We concur.

The campus will, by April 2009, perform an assessment of business need for local administrative accounts and disable unnecessary privileges to restrict the use of unauthorized software.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

Recommendation 22

We recommend that the campus repair all of the network device vulnerabilities that were identified and presented in detail to the campus.

In addition, we recommend that the campus formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.

Campus Response

We concur.

The campus repaired or remediated all of the network device vulnerabilities that were identified and presented to the campus by August 2008.

The campus will, by April 2009, create a documented security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment, and mitigate network device vulnerabilities that were identified and presented in detail to the campus.

OTHER NETWORK DEVICES

Recommendation 23

We recommend that campus:

- a. Assess the security posture of identified modems to ensure the modems are properly secured.
- b. Document the periodic assessment of unauthorized wireless access points.
- c. Perform and document an assessment of risks related to the accessibility of printers via web interface.

Campus Response

We concur.

The campus will, by March 2009:

- assess the security posture of identified modems to ensure the modems are properly secured
- document the periodic assessment of unauthorized wireless access points
- perform and document an assessment of risks related to the accessibility of printers via web interface.

NETWORK ARCHITECTURE

Recommendation 24

We recommend that the campus review its current network topology and determine if Internet accessible devices should be logically separated from devices residing within the internal network.

Campus Response

We concur.

The campus will, by April 2009, review its current network topology and determine if Internet accessible devices should be logically separated from devices residing within the internal network.

REVIEW OF SECURITY EVENT LOGS

Recommendation 25

We recommend that the campus:

- a. Establish a formal process to regularly review and analyze the security logging data to assist in identifying potential network vulnerabilities and breaches on campus systems. This process could include the use of tools and analytical methods, defining personnel responsibilities, reviewing frequency, and reporting/escalating processes.
- b. At a minimum, copy the critical logs to an ancillary server so that they can be retained for an appropriate time frame and be available for subsequent review if needed.

Campus Response

We concur.

The campus will create a policy and procedures to regularly review and analyze security logging data to assist in identifying potential network vulnerabilities and breaches on campus systems by March 2009. These policies and procedures will include the use of tools and analytical methods, defining personnel responsibilities, review frequency, and reporting/escalating processes. The policy and procedures will include copying critical logs to an ancillary server so that they can be retained for an appropriate time frame and be available for subsequent review if needed.

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

Recommendation 26

We recommend that the campus:

- a. Conduct an assessment of all campus computers to ensure security of protected information.



- b. Revise the current data classification policy to provide guidance on the storage and transmission of sensitive information.

Campus Response

We concur.

The campus will revise the current data classification policy to provide guidance on the storage and transmission of Protected Level 1 information and conduct a survey of campus desktop users to identify and secure systems with Protected Level 1 information by March 2009.

THREAT MANAGEMENT

Recommendation 27

We recommend the campus implement an intrusion detection system to monitor and respond to potential security threats.

Campus Response

We concur.

The campus will implement a host (desktop and server) based intrusion detection system to monitor and respond to potential security threats by March 2009. The campus will also develop a plan for implementation of the Juniper network based intrusion detection system by March 2009.

LOST/STOLEN COMPUTERS

Recommendation 28

We recommend that the campus develop and implement a computer loss-theft checklist to ensure that the investigation and certification of possible protected data on lost/stolen computers is sufficiently documented and retained.

Campus Response

We concur.

The campus will develop and implement a computer loss-theft checklist to ensure that the investigation and certification of possible protected data on lost or stolen computers is sufficiently documented and retained by December 2008.





THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

January 26, 2009

CHANNEL ISLANDS

CHICO

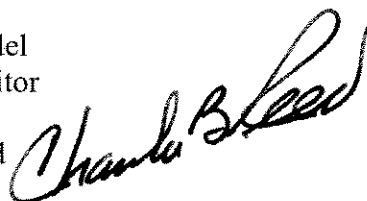
MEMORANDUM

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed
Chancellor


FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 08-19 on *Information Security*,
California State University, Chico

LONG BEACH

LOS ANGELES

In response to your memorandum of January 26, 2009, I accept the response as submitted with the draft final report on *Information Security*, California State University, Chico.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/jt

POMONA

Enclosure

SACRAMENTO

cc: Ms. Lorraine B. Hoffman, Vice President, Business and Finance
Dr. Paul J. Zingg, President

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS

