

**INFORMATION SECURITY
SAN JOSÉ STATE UNIVERSITY**

**Audit Report 08-20
March 4, 2009**

Members, Committee on Audit

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

Staff

University Auditor: Larry Mandel
Senior Director: Michelle Schlack
IT Audit Manager: Greg Dove
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 Organization	8
Policy Issuance and Approval	9
Security Authority and Responsibility	9
Information Security Plan.....	10
Payment Card Industry Data Security Standard.....	11
Record Retention	11
Employee Separation.....	12
Information Security Awareness Training.....	13
Decentralized Computing	13
Server Environments	13
Technical Vulnerabilities.....	14
System Development and Change Management.....	15
Systems Security and Monitoring	16
Configuration Changes	16
Network Countermeasures	17
Network Monitoring.....	18
Vulnerability Management.....	18
Password Standards.....	19
Granting of Administrative Access	20
Firewalls and Routing and Switching Devices.....	20
Network Architecture	21
Other Network Devices	22
Review of Security Event Logs.....	22
Operating Systems Vulnerabilities	23
Protected Data	24
Assessment and Inventory of Protected Information.....	24
Lost/Stolen Computers	25
Disposition of Protected Data.....	26

APPENDICES

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

ABBREVIATIONS

CIO	Chief Information Officer
CISC	Campus Information Security Committee
CSU	California State University
DMZ	Demilitarized Zone
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
PCI DSS	Payment Card Industry Data Security Standard
UCAT	University Computing and Telecommunications
UIT	University Information Technology

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 San José State University campus from September 2, 2008, through October 10, 2008, and audited the procedures in effect at that time.

Our study and evaluation identified issues that, if left unattended, could 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 October 10, 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 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 administration of the campus information security committee required improvement. The process to review, update, and approve information security policies, procedures, and guidelines was deficient. The campus did not have a full-time information security officer. The campus lacked a formal process to identify and prioritize information security risks and create an action plan to adequately address identified risks within an established timeline. Not all auxiliaries had completed a Payment Card Industry Data Security Standard compliance summary plan to determine their vendor level and corresponding

contractual requirements. The campus record retention action plan required improvement. Specifically, the campus did not have comprehensive written documentation formally designating its custodian of records. Employees were not reminded of their ongoing legal responsibility for maintaining the security of protected data at the time of their separation. The campus did not provide information security awareness training to all employees with key responsibilities for maintaining IT security.

DECENTRALIZED COMPUTING [13]

Administration of decentralized departmental server environments required improvement. Technical vulnerabilities existed on a variety of decentralized systems throughout the campus.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [15]

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

SYSTEM SECURITY AND MONITORING [16]

The campus lacked policies and procedures that defined a formal periodic review of configuration changes. The campus had not implemented the use of network countermeasures to deter malicious Internet traffic and reconnaissance attempts. 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 ancillary IT groups. The campus lacked a standard process to detect vulnerabilities or exploits related to security of servers and desktops connected to the campus network. The campus lacked a standard password policy, and password best practices were not consistently enforced. The campus lacked a formal process for granting privileged access to accounts. Firewalls and routing and switching devices were not always properly configured or adequately secured. Internet-accessible devices were located within the same segments as internal resources. The campus had not identified the security risks of modems attached to the network. The campus lacked a formal process for the review of security event logs. Technical vulnerabilities existed on selected operating systems.

PROTECTED DATA [24]

The campus had not conducted an overall security assessment of desktops with sensitive information, and the data classification policy required improvement. The process to report lost/stolen equipment to the information security office to ensure the disposition of sensitive equipment required improvement. Procedures to ensure that all sensitive information on computers was properly deleted prior to disposition required improvement.

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 San José State University, the office of information technology services 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 San José State University 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 applications 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 ORGANIZATION

The administration of the campus information security committee (CISC) required improvement.

We found that:

- ▶ Committee meeting minutes were not consistently completed.
- ▶ Security incidents and project status were not consistently reported to the CISC to ensure appropriate follow-up and disposition.
- ▶ Policies, procedures, and guidelines issued from CISC were not consistently communicated to the various departments on campus to ensure compliance.
- ▶ Auxiliary groups had not been included as part of the CISC group to ensure appropriate campus representation on the committee.

The director of internal control stated that the CISC was recently implemented and its structure was not completely in place.

Failure to appropriately manage information security activities increases the risk of misunderstandings and does not ensure that security activities are being implemented in accordance with management intent.

Recommendation 1

We recommend that the campus:

- a. Timely complete CISC meeting minutes.
- b. Report all security incidents and project status to the CISC.
- c. Communicate CISC policies, procedures, and guidelines to all campus departments.
- d. Include auxiliary groups as part of the CISC.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to:

- a. Timely complete CISC meeting minutes.
- b. Report all security incidents and project status to the CISC.
- c. Communicate CISC policies, procedures, and guidelines to all campus departments.
- d. Include auxiliary groups as part of the CISC.

POLICY ISSUANCE AND APPROVAL

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

We noted that:

- ▶ The Acceptable Use policy delegated responsibility for monitoring and ensuring compliance with the policy to university information technology (UIT); however, UIT was dissolved February 28, 2005.
- ▶ The Privacy of Electronic Communication policy delegated responsibility for implementing policies and procedures to the chief information officer (CIO); however, the CIO position was dissolved May 1, 2000. In addition, the policy had not been reviewed to determine whether it conflicted with current e-mail record retention guidelines.
- ▶ Various policies, procedures, and guidelines were in draft form and did not reflect any documented approval by management.

The director of internal control stated that there was a lapse in campus assignment of university-wide responsibilities for information technology (IT) policies in 2004, 2005, and 2006.

Failure to properly review, update, and approve information security policies, practices, and guidelines limits the effectiveness of information security governance.

Recommendation 2

We recommend that the campus develop a process to ensure that information security policies, procedures, and guidelines are periodically reviewed, updated, and formally approved.

Campus Response

We concur. We will complete management remedial action by the end of July 2009 to develop a process to ensure that information security policies, procedures, and guidelines are periodically reviewed, updated, and formally approved.

SECURITY AUTHORITY AND RESPONSIBILITY

The campus did not have a full-time information security officer.

We noted that the campus designated information security officer was allocated only 33 percent of his time for the information security function.

The vice president of administration and finance stated that these duties had been assumed by the director of internal control and his responsibilities related to information security were limited to coordinating and working with information security policies and procedures.

The lack of a full-time information security officer limits the campus' ability to direct a comprehensive system of information security management throughout the campus community, consistently apply security governance, and prioritize information security prerogatives.

Recommendation 3

We recommend that the campus appoint a full-time information security officer dedicated to fulfilling information security responsibilities.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 regarding the requirement to have a full-time information security officer dedicated to fulfilling information security responsibilities.

INFORMATION SECURITY PLAN

The campus lacked a formal process to identify and prioritize information security risks and create an action plan to adequately address identified risks within an established timeline.

The director of internal control stated that although the CISC required periodic project reporting by various departments, it had not developed an action plan to prioritize and address identified risks within an established timeline.

The lack of a formal process to identify and prioritize information security risks and create an action plan to adequately address identified risks within an established timeline increases the risk of misunderstandings regarding campus information security risks and impacts the campus' ability to opine on the overall effectiveness of existing security provisions related to protected data.

Recommendation 4

We recommend that the campus establish a formal process to identify and prioritize information security risks and create an action plan to adequately address identified risks within an established timeline.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to establish a formal process to identify and prioritize information security risks and create an action plan to adequately address identified risks within an established timeline.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Not all auxiliaries had completed a Payment Card Industry Data Security Standard (PCI DSS) compliance summary plan to determine their vendor level and corresponding 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 network as required by PCI DSS.
- ▶ Responsibility for assessing auxiliary PCI DSS compliance was not defined.

The director of internal control stated that although the campus and most auxiliaries had started and/or completed a PCI DSS compliance review, one auxiliary had yet to comply.

Failure to comply with PCI DSS requirements exposes the auxiliary to potential financial penalties and credit card usage restrictions, which could include termination of the auxiliaries' ability to accept credit cards.

Recommendation 5

We recommend that the campus:

- a. Ensure that the auxiliary completes a PCI assessment to determine its applicable vendor level and respective PCI requirements.
- b. Define and document responsibility for assessing auxiliary PCI DSS compliance.

Campus Response

We concur. We will complete management remedial action by the end of July 2009 to:

- a. Ensure that the auxiliary completes a PCI assessment to determine its applicable vendor level and respective PCI requirements.
- b. Define and document responsibility for assessing auxiliary PCI DSS compliance.

RECORD RETENTION

The campus record retention action plan required improvement.

Specifically, we noted that the campus did not have comprehensive written documentation formally designating its custodians of records.

Executive Order 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 director of internal control stated his belief that many custodians of records had been designated based on their job functions and that no separate written designation was necessary.

Failure to formally designate custodians of records increases the risk of misunderstandings and may result in operational inefficiencies and inconsistent record retention practices across the California State University (CSU).

Recommendation 6

We recommend that the campus revise its record retention action plan to formally designate its custodians of records and to ensure appropriate and timely disposal of records/information in accordance with CSU record retention and disposition schedules.

Campus Response

We concur. We will complete management remedial action by the end of June 2009 to revise the record retention action plan to formally designate its custodians of records and to ensure appropriate and timely disposal of records/information in accordance with CSU record retention and disposition schedules.

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 director of internal control stated his belief that such a reminder is already implicit in the 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 its personnel 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. We will complete management remedial action by the end of June 2009 to modify the personnel exit process to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data.

INFORMATION SECURITY AWARENESS TRAINING

The campus did not provide information security awareness training to all employees with key responsibilities for maintaining IT security.

The director of internal control stated that phase one deployment of security awareness training was supposed to capture all key IT personnel but some people had not been trained due to omission.

Failure to provide employees with information security awareness training increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.

Recommendation 8

We recommend that the campus develop and implement an information security awareness training program for all employees, especially for those with access to critical systems or protected data.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to develop and implement an information security awareness training program for all employees, especially for those with access to critical systems or protected data.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Administration of decentralized departmental server environments required improvement.

Our review of three departments disclosed that:

- ▶ In one department, general privilege user accounts were being shared among IT personnel.
- ▶ Web servers hosted by one department were not subject to web accessibility controls.
- ▶ E-mail retention schedules were not in place for all three departments with e-mail servers.

The director of internal control stated that department system owners and server administrators were responsible for securing their own systems and that best practice might not have been followed.

Failure to effectively administer decentralized servers increases the risk that servers may be compromised, resulting in loss of confidential data in the event of a security breach.

Recommendation 9

We recommend that the campus implement procedures to ensure that:

- a. Privileged user accounts are not being shared among users.
- b. Web pages hosted on various department servers are subject to accessibility controls.
- c. E-mail retention schedules are consistent for all e-mail servers on campus.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to ensure that:

- a. Privileged user accounts are not being shared among users.
- b. Web pages hosted on various department servers are subject to accessibility controls.
- c. E-mail retention schedules are consistent for all e-mail servers on campus.

TECHNICAL VULNERABILITIES

Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the central IT team and were not held to the same programming standard and code review or security configuration standards.

Our external testing of selected servers disclosed 124 vulnerabilities on a variety of servers for which specific details were provided to the campus.

Additionally, deployment of servers in the decentralized computing environment was unmanaged and lacked professional standards and guidance. The 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 director of internal control stated that control and oversight was incomplete due to decentralization of IT.

Server vulnerabilities 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. 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.
- c. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the ancillary IT units with a security baseline standard for securing servers.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to ensure that the identified technical vulnerabilities are repaired; in addition, we will:

- 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. 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.
- c. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the ancillary IT units with a security baseline standard for securing servers.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

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

The web application we reviewed allowed improper permissions to file/directory, the Autocomplete attribute for user credentials, secured page browser cache, login error credential enumeration, and Structured Query Language injection fingerprinting.

The senior director of administrative systems stated that the system was designed by a third-party consultant before web vulnerabilities were widely known and it has been maintained locally; however, there is no centralized process on campus to perform vulnerability testing nor a consolidated center of knowledge on how to identify and resolve vulnerabilities. He also stated that server patching on production applications requires thorough testing prior to applying operating system patches to ensure that the patch will not inadvertently disable a production system.

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 11

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 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. We will complete management remedial action by the end of August 2009 to ensure that the identified technical vulnerabilities are repaired; in addition, we will:

- a. Formalize a security 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.

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 systems and devices informally occurred at regular intervals 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 interim associate vice president of university computing and telecommunications (UCAT) stated that the campus had not considered it necessary 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 12

We recommend that the campus:

- a. Develop policies and procedures and establish a formal process for the periodic review of system configurations that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.
- b. Incorporate into these formal change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance of configuration reviews.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to:

- a. Develop policies and procedures and establish a formal process for the periodic review of system configurations that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.
- b. Incorporate into these formal change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance of configuration reviews.

NETWORK COUNTERMEASURES

The campus had not implemented the use of network countermeasures to deter malicious Internet traffic and reconnaissance attempts.

The interim associate vice president of UCAT stated that the campus had not implemented such countermeasures due to resource constraints.

Failure to effectively shield the network from active traffic analysis attacks may lead to compromise in network resources and loss of protected confidential information.

Recommendation 13

We recommend that the campus implement active countermeasures on the network, such as ingress throttling of malicious traffic.

Campus Response

We concur. We will complete management remedial action by the end of July 2009 to implement active countermeasures on the network, such as ingress throttling of malicious traffic.

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 ancillary IT groups.

The interim associate vice president of UCAT stated that although there was a process to identify externally facing web servers, the process was not formalized and did not identify all servers on campus.

The inability to identify and monitor all campus IT resources (servers, workstations, and laptops) can leave the campus 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 14

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. We will complete management remedial action by the end of August 2009 to:

- 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.

VULNERABILITY MANAGEMENT

The campus lacked a standard process to detect vulnerabilities or exploits related to security of servers and desktops connected to the campus network.

Detection processes were performed intermittently by different divisions to varying degrees; however, there was no consistent standard to detect campus-wide vulnerabilities and exploits to ensure compliance with campus-wide policies.

The interim associate vice president of UCAT stated that although a vulnerability assessment had been performed in 2006, a standard process to periodically scan servers and desktops connected to the campus network had not been implemented.

Failure to adequately identify vulnerabilities and exploits may lead to compromise in network resources and loss of protected confidential information.

Recommendation 15

We recommend that the campus develop a consistent process to detect vulnerabilities and exploits on all servers and desktops connected to the campus network.

Campus Response

We concur. We will complete management remedial action by the end of July 2009 to develop a consistent process to detect vulnerabilities and exploits on all servers and desktops connected to the campus network.

PASSWORD STANDARDS

The campus lacked a standard password policy, and password best practices were not consistently enforced.

We noted inconsistencies in the implementation of password best practices in various departments on campus.

The director of internal control stated that the decentralized nature of campus departments made it difficult to enforce password best practices. He further stated that individual departments were responsible for implementing password standardization and that password policy was not deemed to be a top priority.

The lack of a standard enforced password policy for critical applications increases the risk for both easily guessed passwords and possible unauthorized access to network resources and confidential information.

Recommendation 16

We recommend the campus implement a standard password policy and ensure that all departments comply with the policy.

Campus Response

We concur. We will complete management remedial action by the end of June 2009 to implement a standard password policy and ensure that all departments comply with the policy.

GRANTING OF ADMINISTRATIVE ACCESS

The campus lacked a formal process for granting privileged access to accounts.

The interim associate vice president of UCAT stated that the number of people with privileged access to accounts was limited, and therefore, he did not believe a formal process was necessary.

The lack of a formal process for granting privileged access may lead to inadequate segregation of duties, the granting of accounts not based on the principle of least privilege, and/or unauthorized access.

Recommendation 17

We recommend that the campus establish a formal process 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.

Campus Response

We concur. We will complete management remedial action by the end of July 2009 to establish a formal process 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.

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:

- ▶ Five devices and the border firewall were configured with Simple Network Management Protocol, which was unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ Six devices were enabled with Telecommunication Network, which could allow a remote attacker to obtain confidential authentication tokens to permit remote access to the devices since the user logins, passwords, and commands are transferred across the network in clear text.

- ▶ Six devices were 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.
- ▶ Three devices were configured without management host address restrictions, which could allow any attacker to connect to the HTTPS service and logon.

The interim associate vice president of UCAT stated that these vulnerabilities were due to configuration mistakes by staff.

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 18

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:

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

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to:

- a. Repair all of the network device vulnerabilities that were identified and presented to the campus.
- c. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- d. Implement a comprehensive, campus-wide patch management process.

NETWORK ARCHITECTURE

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

The interim associate vice president of UCAT 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 19

We recommend that the campus review its current network topology and determine how to best logically separate Internet-accessible devices from devices residing within the internal network.

Campus Response

We concur. We will complete management remedial action by the end of July 2009 to review the current network topology and determine how to best logically separate Internet-accessible devices from devices residing within the internal network.

OTHER NETWORK DEVICES

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

The interim associate vice president of UCAT stated that the lack of modem security review was an oversight.

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

Recommendation 20

We recommend that campus assess the security posture of modems attached to the network and ensure that the modems are properly secured.

Campus Response

We concur. We will complete management remedial action by the end of June 2009 to assess the security posture of modems attached to the network and ensure that the modems are properly secured.

REVIEW OF SECURITY EVENT LOGS

The campus lacked a formal process for the review of security event logs.

We noted that security event log reviews were informally performed and undocumented.

The interim associate vice president of UCAT stated that resource constraints limited the amount of time that personnel could spend manually reviewing security event logs.

Inadequate review of security event 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, which could lead to confidential information being breached and not reported.

Recommendation 21

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. Consider the implementation of centralized security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to:

- 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.
- b. Consider the implementation of centralized security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

OPERATING SYSTEMS VULNERABILITIES

Technical vulnerabilities existed on selected operating systems.

Our testing of selected servers disclosed the various vulnerabilities for which specific details were provided to the campus. Ten servers were running vulnerable versions of remote desktop protocol, two servers were running remote Oracle Listener Program with no passwords assigned, two servers were vulnerable to mail relay, two servers were running a vulnerable version of storage manager client, and one server was running a vulnerable version of Lotus Domino.

The interim associate vice president of UCAT stated that these vulnerabilities were the result of various causes, including programming oversight and delays in patching servers and/or applications.

These vulnerabilities increase the risk of a remote attack 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 22

We recommend that the campus repair all the technical 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 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. We will complete management remedial action by the end of July 2009 to:

- a. Repair all the technical vulnerabilities that were identified and presented in detail to the campus.
- b. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.
- c. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

The campus had not conducted an overall security assessment of desktops with sensitive information, and the data classification policy required improvement.

Specifically, the current data classification policy did not provide guidance on the handling of sensitive information in certain situations related to various forms of media (i.e., removable media, electronic communications, etc.).

The director of internal control stated that the campus was in the process of defining data classification standards and had yet to conduct an overall assessment of desktops with sensitive information.

Inadequate accountability of assets, especially those containing personal confidential information or with accessibility to such protected information, increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

Recommendation 23

We recommend that the campus:

- a. Conduct an assessment of the current inventory and security of protected information.
- b. Revise the current data classification policy to provide guidance on the handling of sensitive information stored on various forms of media.

Campus Response

We concur. We will complete management remedial action by the end of August 2009 to:

- a. Conduct an assessment of the current inventory and security of protected information.
- b. Revise the current data classification policy to provide guidance on the handling of sensitive information stored on various forms of media.

LOST/STOLEN COMPUTERS

The process to report lost/stolen equipment to the information security office to ensure the disposition of sensitive equipment required improvement.

We noted several instances where lost/stolen computers had not been investigated by the information security office.

The director of internal control stated that the university police department was responsible for notifying the information security office of any lost/stolen equipment but this practice was not consistently followed.

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 24

We recommend that the campus develop and implement a computer loss/theft checklist to ensure that the investigation and certification of the existence of protected data is sufficiently documented and retained.

Campus Response

We concur. We will complete management remedial action by the end of June 2009 to develop and implement a computer loss/theft checklist to ensure that the investigation and certification of the existence of protected data is sufficiently documented and retained.

DISPOSITION OF PROTECTED DATA

Procedures to ensure that all sensitive information on computers was properly deleted prior to disposition required improvement.

Specifically, the campus lacked a formal process to ensure and document hard-drive wiping.

The director of internal control stated that although a revised and improved process was put into place, it did not require formal sign-off by IT support.

Inadequate control over equipment assets, especially those containing personal confidential information, increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

Recommendation 25

We recommend that the campus update its campus property survey forms to ensure that hard-drive wiping is performed and sufficiently documented, including retention of the documentation.

Campus Response

We concur. We will complete management remedial action by the end of June 2009 to update the campus property survey forms to ensure that hard-drive wiping is performed and sufficiently documented, including retention of the documentation.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Jon Whitmore	President
Ruben Araiza	Property Coordinator
Don Baker	Interim Associate Vice President, University Computing and Telecommunications (UCAT)
Mike Dunefsky	Senior Director, Administrative Systems
Farukh Farid	Library Information Technology Manager
Bruce Gardner	Operating Systems Analyst
Mary Jo Gorney-Moreno	Associate Vice President, Academic Technology
David Kessler	Network Analyst, College of Applied Science and Arts
Cathy Kozak	Network Analyst, College of Science
Christopher Laxton	Director of Media Production and Delivery, TV Education Network
Rose Lee	Vice President, Administration and Finance
Ninh Pham-Hi	Director of Internal Control
Richard Porter	Network Analyst, UCAT
Maria Rivera	Associate Vice President of Human Resources
Rigoberto Vargas	Information Technology Consultant, University Advancement
Ronald Wong	Information Technology Consultant, College of Business
Rong Wong	Network Analyst, UCAT



San José State
UNIVERSITY

**Office of the Vice President
for Administration and
Finance**

One Washington Square
San José, CA 95192-0006
Voice: 408-924-1500
Fax: 408-924-1515
<http://www.sjsu.edu>

April 13, 2009

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

RECEIVED
UNIVERSITY AUDITOR

APR - 8 2009

THE CALIFORNIA STATE
UNIVERSITY

**Campus Response to INFORMATION SECURITY AUDIT (#08-20) at
San José State University**

Enclosed is San José State University's response to the Information Security Audit. The campus is committed to addressing the issues identified in this audit report.

Please let me know if I can provide you with additional information.

Rose L. Lee

ROSE L. LEE
Vice President for Administration and Finance

Enclosure

cc: Jon Whitmore, President
Ninh Pham-Hi, Director, Internal Control

The California State University:

Chancellor's Office, Bakersfield, Channel Islands, Chico, Dominguez Hills, East Bay, Fresno, Fullerton, Humboldt, Long Beach, Los Angeles, Maritime Academy, Monterey Bay, Northridge, Pomona, Sacramento, San Bernardino, San Diego, San Francisco, San José, San Louis Obispo, San Marcos, Sonoma, Stanislaus

INFORMATION SECURITY
SAN JOSÉ STATE UNIVERSITY
Audit Report 08-20

SECURITY GOVERNANCE

SECURITY ORGANIZATION

Recommendation 1

We recommend that the campus:

- a. Timely complete CISC meeting minutes.
- b. Report all security incidents and project status to the CISC.
- c. Communicate CISC policies, procedures, and guidelines to all campus departments.
- d. Include auxiliary groups as part of the CISC.

Campus Response

We concur. We will complete management remedial action to (a) Timely complete CISC meeting minutes. (b) Report all security incidents and project status to the CISC. (c) Communicate CISC policies, procedures, and guidelines to all campus departments. (d) Include auxiliary groups as part of the CISC. By end of August 09.

POLICY ISSUANCE AND APPROVAL

Recommendation 2

We recommend that the campus develop a process to ensure that information security policies, procedures, and guidelines are periodically reviewed, updated, and formally approved.

Campus Response

We concur. We will complete management remedial action to develop a process to ensure that information security policies, procedures, and guidelines are periodically reviewed, updated, and formally approved. By end of July 09.

SECURITY AUTHORITY AND RESPONSIBILITY

Recommendation 3

We recommend that the campus appoint a full-time information security officer dedicated to fulfilling information security responsibilities.

Campus Response

We concur. We will complete management remedial action regarding the requirement to have a full-time information security officer dedicated to fulfilling information security responsibilities. By end of August 09.

INFORMATION SECURITY PLAN**Recommendation 4**

We recommend that the campus establish a formal process to identify and prioritize information security risks and create an action plan to adequately address identified risks within an established timeline.

Campus Response

We concur. We will complete management remedial action to establish a formal process to identify and prioritize information security risks and create an action plan to adequately address identified risks within an established timeline. By August 09.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD**Recommendation 5**

We recommend that the campus:

- a. Ensure that the auxiliary completes a PCI assessment to determine its applicable vendor level and respective PCI requirements.
- b. Define and document responsibility for assessing auxiliary PCI DSS compliance.

Campus Response

We concur. We will complete management remedial action by end of July 09 to:

- a. Ensure that the auxiliary completes a PCI assessment to determine its applicable vendor level and respective PCI requirements.
- b. Define and document responsibility for assessing auxiliary PCI DSS compliance.

RECORD RETENTION**Recommendation 6**

We recommend that the campus revise its record retention action plan to formally designate its custodians of records and to ensure appropriate and timely disposal of records/information in accordance with CSU record retention and disposition schedules.

Campus Response

We concur. We will complete management remedial action to revise the record retention action plan to formally designate its custodians of records and to ensure appropriate and timely disposal of records/information in accordance with CSU record retention and disposition schedules. By end of June 09.

EMPLOYEE SEPARATION

Recommendation 7

We recommend that the campus modify its personnel 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. We will complete management remedial action to modify the personnel exit process to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data. By end of June 09.

INFORMATION SECURITY AWARENESS TRAINING

Recommendation 8

We recommend that the campus develop and implement an information security awareness training program for all employees, especially for those with access to critical systems or protected data.

Campus Response

We concur. We will complete management remedial action to develop and implement an information security awareness training program for all employees, especially for those with access to critical systems or protected data. By end of August 09.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Recommendation 9

We recommend that the campus implement procedures to ensure that:

- a. Privileged user accounts are not being shared among users.
- b. Web pages hosted on various department servers are subject to accessibility controls.
- c. E-mail retention schedules are consistent for all e-mail servers on campus.

Campus Response

We concur. We will complete management remedial action by end of August 09 to ensure that:

- a. Privileged user accounts are not being shared among users.
- b. Web pages hosted on various department servers are subject to accessibility controls.
- c. E-mail retention schedules are consistent for all e-mail servers on campus.

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. 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.
- c. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the ancillary IT units with a security baseline standard for securing servers.

Campus Response

We concur. We will complete management remedial action by end of August 09 to ensure that the identified technical vulnerabilities are repaired; in addition, we will:

- 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. 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.
- c. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the ancillary IT units with a security baseline standard for securing servers.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

Recommendation 11

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 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. We will complete management remedial action by end of August 09 to ensure that the identified technical vulnerabilities are repaired; in addition, we will:

- a. Formalize a security 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.

SYSTEMS SECURITY AND MONITORING

CONFIGURATION CHANGES

Recommendation 12

We recommend that the campus:

- a. Develop policies and procedures and establish a formal process for the periodic review of system configurations that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.
- b. Incorporate into these formal change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance of configuration reviews.

Campus Response

We concur. We will complete management remedial action by end of August 09 to:

- a. Develop policies and procedures and establish a formal process for the periodic review of system configurations that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.
- b. Incorporate into these formal change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance of configuration reviews.

NETWORK COUNTERMEASURES

Recommendation 13

We recommend that the campus implement active countermeasures on the network, such as ingress throttling of malicious traffic.

Campus Response

We concur. We will complete management remedial action by end of July 09 to implement active countermeasures on the network, such as ingress throttling of malicious traffic.

NETWORK MONITORING

Recommendation 14

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. We will complete management remedial action by end of August 09 to:

- 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.

VULNERABILITY MANAGEMENT

Recommendation 15

We recommend that the campus develop a consistent process to detect vulnerabilities and exploits on all servers and desktops connected to the campus network.

Campus Response

We concur. We will complete management remedial action by end of July 09 to develop a consistent process to detect vulnerabilities and exploits on all servers and desktops connected to the campus network.

PASSWORD STANDARDS

Recommendation 16

We recommend the campus implement a standard password policy and ensure that all departments comply with the policy.

Campus Response

We concur. We will complete management remedial action by end of June 09 to implement a standard password policy and ensure that all departments comply with the policy.

GRANTING OF ADMINISTRATIVE ACCESS

Recommendation 17

We recommend that the campus establish a formal process 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.

Campus Response

We concur. We will complete management remedial action by end of July 09 to establish a formal process 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.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

Recommendation 18

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:

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

Campus Response

We concur. We will complete management remedial action by end of August 09 to:

- a. Repair all of the network device vulnerabilities that were identified and presented to the campus.
- b. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- c. Implement a comprehensive, campus-wide patch management process.

NETWORK ARCHITECTURE

Recommendation 19

We recommend that the campus review its current network topology and determine how to best logically separate Internet-accessible devices from devices residing within the internal network.

Campus Response

We concur. We will complete management remedial action by end of July 09 to review the current network topology and determine how to best logically separate Internet-accessible devices from devices residing within the internal network.

OTHER NETWORK DEVICES

Recommendation 20

We recommend that campus assess the security posture of modems attached to the network and ensure that the modems are properly secured.

Campus Response

We concur. We will complete management remedial action by end of June 09 to assess the security posture of modems attached to the network and ensure that the modems are properly secured.

REVIEW OF SECURITY EVENT LOGS

Recommendation 21

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. Consider the implementation of centralized security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

Campus Response

We concur. We will complete management remedial action by end of August 09 to:

- 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.
- b. Consider the implementation of centralized security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

OPERATING SYSTEMS VULNERABILITIES

Recommendation 22

We recommend that the campus repair all the technical 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 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. We will complete management remedial action by end of July 09 to:

- a. Repair all the technical vulnerabilities that were identified and presented in detail to the campus

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

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

Recommendation 23

We recommend that the campus:

- a. Conduct an assessment of the current inventory and security of protected information.
- b. Revise the current data classification policy to provide guidance on the handling of sensitive information stored on various forms of media.

Campus Response

We concur. We will complete management remedial action by end of August 09 to:

- a. Conduct an assessment of the current inventory and security of protected information.
- b. Revise the current data classification policy to provide guidance on the handling of sensitive information stored on various forms of media.

LOST/STOLEN COMPUTERS

Recommendation 24

We recommend that the campus develop and implement a computer loss/theft checklist to ensure that the investigation and certification of the existence of protected data is sufficiently documented and retained.

Campus Response

We concur. We will complete management remedial action by end of June 09 to develop and implement a computer loss/theft checklist to ensure that the investigation and certification of the existence of protected data is sufficiently documented and retained.

DISPOSITION OF PROTECTED DATA

Recommendation 25

We recommend that the campus update its campus property survey forms to ensure that hard-drive wiping is performed and sufficiently documented, including retention of the documentation.

Campus Response

We concur. We will complete management remedial action by end of June 09 to update the campus property survey forms to ensure that hard-drive wiping is performed and sufficiently documented, including retention of the documentation.



THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

May 5, 2009

CHANNEL ISLANDS

CHICO

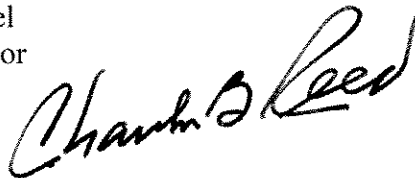
MEMORANDUM

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed
Chancellor


FULLERTON

SUBJECT: Draft Final Report 08-20 on *Information Security*,
San José State University

HUMBOLDT

LONG BEACH

In response to your memorandum of May 5, 2009, I accept the response as submitted with the draft final report on *Information Security*, San José State University.

LOS ANGELES

MARITIME ACADEMY

MONTEREY BAY

CBR/amd

NORTHRIDGE

Enclosure

POMONA

c: Ms. Rose L. Lee, Vice President, Administration and Finance
Dr. Jon Whitmore, President

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS