

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
CHANNEL ISLANDS

Audit Report 09-37
January 28, 2010

Members, Committee on Audit

Melinda Guzman, Chair
Raymond W. Holdsworth, Vice Chair
Herbert L. Carter Carol R. Chandler
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

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
Information Security Plan	8
Use of Employee-Owned Computers.....	9
Employee Separation	9
Systems Security and Monitoring	10
Technical Vulnerabilities.....	10
Website Vulnerability Management	11
Configuration Changes	11
Vulnerability Management	12
Password Standards	13
Granting of Administrative Access.....	13
Firewalls and Routing and Switching Devices	14
Network Architecture	15
Review of Security Event Logs	15
Protected Data.....	16
System Backup Encryption.....	16
Incident Response Management	17

APPENDICES

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

ABBREVIATIONS

CIO	Chief Information Officer
CSU	California State University
CSUCI	California State University, Channel Islands
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISMS	Information Security Management System
IT	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 California State University, Channel Islands campus from June 8, 2009, through July 17, 2009, and audited the procedures in effect at that time.

Our study and evaluation revealed internal control problems or weaknesses that would be considered pervasive in their effects on information security controls. These weaknesses are described in the executive summary and body of this report.

In our opinion, the operational and administrative controls of information security in effect as of July 17, 2009, taken as a whole, were not sufficient to meet the objectives for a secured computing environment. While much of the campus information technology department control environment was satisfactory and provided appropriate safeguards over the critical financial and management systems, the practices of the information security office required improvement and greater 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 campus did not have a full-time, dedicated information security officer. Individuals assuming the functions of the information security officer role lacked clearly defined and documented security responsibilities. The campus had not performed a risk assessment to identify and prioritize all information security risks, did not have a comprehensive action plan to report and monitor security needs, and did not have a formal process for collecting and reporting information security activities to executive management. The campus did not enforce antivirus or patch management solutions for home computers that were used for business purposes and to access the campus network. Employee separation documentation did not include a reminder to the separating party of their ongoing legal responsibility for maintaining the security of protected data.

SYSTEMS SECURITY AND MONITORING [10]

Technical vulnerabilities existed on a variety of systems throughout the campus. Two application vulnerabilities existed on the website selected for testing. The campus lacked policies and procedures that defined a formal periodic review of configuration changes for firewalls, switches, routers, and operating systems. The campus did not actively monitor intrusion security events. In addition, the network security devices were not configured with automated rules to respond to network security events in order to restrict or block traffic from potential security threats. The campus password practices required improvement. The campus lacked a formal process for granting and managing accounts with privileged system-level access. Firewalls and routing and switching devices were not always properly configured or adequately secured. Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources. The campus lacked a formal process for the review of security event logs.

PROTECTED DATA [16]

The full backup files for all campus administrative systems were stored at an off-site location in an unencrypted format. The campus' security incident handling procedures for compromised electronic resources 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; information technology 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. 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, Channel Islands (CSUCI), the office of information technology services has overall responsibility for the management of campus systems and networks.

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 and are equipped to support organizational security policy in the course of their normal work; and procedures are in place to ensure that users' separation 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 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 are identified and addressed.

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 reviewing 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 evaluating 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 retained contractors 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 CSUCI 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's programming.

Our testing and methodology were 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 did not have a full-time, dedicated information security officer. Individuals assuming the functions of the information security officer role lacked clearly defined and documented security responsibilities.

The interim chief information officer (CIO) stated that limited staffing resources precluded staffing this position with a full-time employee. He also stated that the campus had been working to develop an approach to effectively fulfill its information security responsibilities.

The lack of a full-time, dedicated information security officer and clearly defined security responsibilities increases the risk of misunderstandings regarding information security responsibilities. It also 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 1

We recommend that the campus modify its information security organization to ensure that all security initiatives and committees are aligned to create a cohesive security structure that ensures the campus-approved security plan is implemented in accordance with management intent and oversight. We recommend that one person be assigned overall responsibility for information security initiatives.

Campus Response

We agree. The campus will designate one person to have overall responsibility for information security initiatives by July 31, 2010.

INFORMATION SECURITY PLAN

The campus had not performed a risk assessment to identify and prioritize all information security risks, did not have a comprehensive action plan to report and monitor security needs, and did not have a formal process for collecting and reporting information security activities to executive management.

The interim CIO stated that the campus had developed an information security plan to address known risks, but a comprehensive risk assessment was not performed to identify all potential security risks.

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 threats and potential impact. This deficiency could contribute to erroneous management decisions regarding the overall effectiveness of the campus' information security needs and priorities.

Recommendation 2

We recommend that the campus establish a formal risk assessment process to identify and prioritize information security risks, perform a detailed information security risk assessment, and create a formal process for tracking and reporting progress to executive management.

Campus Response

We agree. We are in the process of risk assessment and review and will create a formal process for tracking and reporting progress to executive management at its completion. This will be completed by September 30, 2010.

USE OF EMPLOYEE-OWNED COMPUTERS

The campus did not enforce antivirus or patch management solutions for home computers that were used for business purposes and to access the campus network.

The interim CIO stated that the campus had recently adopted the security policies developed by the chancellor's office, which include use of home computers for business purposes, but they had not yet implemented measures to ensure that such machines are secure and virus free.

A lack of security controls for employee-owned computers that are used for business purposes increases campus exposure to security breaches.

Recommendation 3

We recommend that the campus implement measures to ensure that home computers used for campus business purposes are patched and protected from viruses before granting access to network resources.

Campus Response

We agree. The campus will either implement measures to ensure that home computers used for campus business purposes are patched and protected from viruses or we will not allow home computers to be used for campus business purposes. This will be completed by June 30, 2010.

EMPLOYEE SEPARATION

Employee separation documentation did not include a reminder to the separating party of their ongoing legal responsibility for maintaining the security of protected data.

The interim associate vice president of human resources stated that the campus was unaware of any requirement to remind separated employees of their responsibility to uphold confidentiality agreements.

Failure to notify separating employees of their 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.

Recommendation 4

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

Campus Response

We agree. The campus will include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data by June 30, 2010.

SYSTEMS SECURITY AND MONITORING

TECHNICAL VULNERABILITIES

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

Our external testing of selected servers disclosed four vulnerabilities on a variety of servers. We provided specific details of these vulnerabilities to the campus.

The information technology (IT) infrastructure manager stated that the campus had recently undertaken significant changes to its network and that these issues were an oversight.

Server vulnerabilities increase the risk of a remote attack on the server that could lead to server disablement, loss of protected confidential information, and execution of malicious programs that could disable other network resources.

Recommendation 5

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

Campus Response

We agree. The campus will repair all the technical vulnerabilities that were identified and presented in detail during the exit interview by June 30, 2010.

WEBSITE VULNERABILITY MANAGEMENT

Two application vulnerabilities existed on the website selected for testing.

The manager of IT user services stated that the vulnerabilities were the result of programming oversight.

Web application vulnerabilities increase the risk that a remote attacker may be able to access protected confidential information or execute malicious programs on the server that could disable other network resources.

Recommendation 6

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

In addition, we recommend that the campus implement a management process for periodic review of existing web application code to minimize its potential susceptibility to new vulnerabilities.

Campus Response

We agree. The campus has already repaired the website vulnerabilities that were identified and presented in detail. By June 30, 2010, the campus will implement a management process for an annual review of existing web application code.

CONFIGURATION CHANGES

The campus lacked policies and procedures that defined a formal periodic review of configuration changes for firewalls, switches, routers, and operating systems.

Informal periodic reviews of these systems and devices occurred at regular intervals as part of network operational responsibilities; however, this informal process was not adequate to ensure that these network devices adhered to the latest configuration standards and updates.

The IT infrastructure manager stated that a lack of resources did not allow for a formal periodic review process.

The lack of formal policies and procedures for reviewing system and device configuration changes decreases accountability for changes made to critical assets. This deficiency also increases the risk of inconsistent and deprecated configuration standards, which may permit malicious activity to go undetected.

Recommendation 7

We recommend that the campus:

- a. Develop policies and procedures to establish a formal review of system configurations so that management can determine accountability for potentially misconfigured network devices and assign responsibility for identifying and remediating configuration problems.
- b. Incorporate into these change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance with configuration reviews.

Campus Response

We agree. The campus will develop policies and procedures to establish a formal review of system configurations so that management can determine accountability for potentially misconfigured network devices and assign responsibility for identifying and remediating configuration problems. We will incorporate into these change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance with configuration reviews. This new process and procedure will be in place by August 30, 2010.

VULNERABILITY MANAGEMENT

The campus did not actively monitor intrusion security events. The network security devices lacked automated rules to restrict or block traffic from potential threats in response to network security events.

The IT infrastructure manager stated that server-based intrusion detection had not been implemented due to resource constraints.

Inadequate security incident monitoring and response procedures increase the risk of loss and inappropriate use of state resources. These deficiencies also increase campus exposure to information security breaches.

Recommendation 8

We recommend that the campus implement intrusion detection provisions to monitor and respond to potential security events.

Campus Response

We agree. The campus will implement intrusion detection provisions to monitor and respond to potential security events by June 30, 2010.

PASSWORD STANDARDS

The campus password practices required improvement.

We noted that:

- ▶ The campus had an informal and undocumented process for passwords related to certain administrator accounts that control core network services.
- ▶ In our review of one server selected for testing, 210 of 2650 user accounts had non-expiring passwords.

The IT infrastructure manager stated that the campus had been making significant changes to the network environment and had not recently revisited the password policies on the existing systems.

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

Recommendation 9

We recommend that the campus extend its password policy to all servers and network devices and implement procedures to ensure compliance with the policy.

Campus Response

We agree. The campus will extend its password policy to all servers and network devices and implement procedures to ensure compliance by June 30, 2010.

GRANTING OF ADMINISTRATIVE ACCESS

The campus lacked a formal process for granting and managing accounts with privileged system-level access.

The IT infrastructure manager stated that the campus had used an informal process because it only allowed privileged access to a limited number of people.

The lack of a formal process for the granting and management of 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 10

We recommend that the campus establish a formal process for granting privileged system-level access to accounts and that it develop a method to track, review, and periodically audit this type of access.

Campus Response

We agree. The campus will establish a formal process for granting privileged system-level access to accounts and develop a method to track, review, and periodically audit this type of access by July 31, 2010.

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 selected routing and switching devices disclosed seven vulnerabilities that were provided separately to the campus.

The IT infrastructure manager stated that these vulnerabilities were due to staff oversight or lack of resources to implement the required technology.

These vulnerabilities increase the risk that a remote attacker may be able to exploit network resources, gain access to protected confidential information, or execute malicious programs that could potentially disable other network resources.

Recommendation 11

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

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. Identify potential or known vulnerabilities by extending the patch management process to include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the network environment.

Campus Response

We agree. The network device vulnerabilities that were identified and presented have been repaired. The campus will formalize a baseline standard that requires the review of network devices for

security vulnerabilities prior to deployment, and we will identify potential or known vulnerabilities by extending the patch management process to include the review of existing device configurations on a periodic basis and new configurations prior to deployment into the network by July 31, 2010.

NETWORK ARCHITECTURE

Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources.

Normally, Internet-accessible devices are segmented into a demilitarized zone so that if these devices are compromised, they are separated from other internal network resources.

The IT infrastructure manager stated that the network had been undergoing significant redesign and that this issue would be addressed as part of the ongoing redesign process.

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.

Recommendation 12

We recommend that the campus review its current network topology and determine the most logical way to separate Internet-accessible devices from other devices within the internal network.

Campus Response

We agree. The campus is reviewing our current network topology, and we will determine the most logical way to separate Internet-accessible devices from other devices within the internal network by June 30, 2010.

REVIEW OF SECURITY EVENT LOGS

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

The IT infrastructure manager stated that the campus has large security event logs and that effective reviews would require a log-management tool. He further stated that the campus has discussed acquiring such a tool but has not yet purchased and implemented one.

The lack of periodic, documented reviews 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. This could lead to an unreported breach of confidential information.

Recommendation 13

We recommend that the campus establish a formal regularized process to review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of campus systems. This process could include the use of tools and analytical methods and should define personnel responsibilities, reviewing frequency, and reporting/escalating procedures.

Campus Response

We agree. The campus will establish a formal regularized process to review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of campus systems. The process will include the use of tools and analytical methods and will define personnel responsibilities, reviewing frequency, and reporting/escalating procedures. This will be completed by July 31, 2010.

PROTECTED DATA

SYSTEM BACKUP ENCRYPTION

The full backup files for all campus administrative systems were stored at an off-site location in unencrypted format.

The interim CIO stated that encryption software had been purchased but had not yet been implemented.

Failure to encrypt sensitive information could expose the campus to accidental disclosure.

Recommendation 14

We recommend that the campus encrypt any system backups that contain protected information when stored at off-site locations.

Campus Response

We agree, and this has already been completed. Beginning August 2009, all system backups that are stored at off-site locations are now encrypted.

INCIDENT RESPONSE MANAGEMENT

The campus' security incident handling procedures for compromised electronic resources required improvement.

We found that:

- ▶ The existing help desk support process did not record all security-related events and incidents in a manner that could be easily extracted and reported.
- ▶ The campus had a process for reporting thefts to the university police department, but that process did not include a directive to report security incidents to the information security office.

The interim CIO stated that this oversight was due to the lack of a full-time security officer to examine existing procedures for effectiveness.

Failure to ensure that the information security incidents are appropriately recorded, monitored, and reported in a consistent manner weakens the campus security posture and increases the risk that compromised systems could inadvertently affect the campus network environment.

Recommendation 15

We recommend that the campus:

- a. Implement a method to consistently record all information security-related incidents.
- b. Enhance its reporting process to ensure that the information security officer is notified of all computer security incidents reported to the university police department.

Campus Response

We agree. The campus will implement a method to consistently record all information security-related incidents and make sure that the information security officer is notified of all computer security incidents reported to the university police department by July 31, 2010.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Richard R. Rush	President
Herbert Aquino	Information Technology (IT) Infrastructure Manager
Michael Berman	Interim Chief Information Officer
Noel Buena	Property Coordinator
Joanne Coville	Vice President, Finance and Administration
Emily Deakin	Controller
Marc Dubransky	Senior Systems Administrator
Neal Fisch	Director, Application Solution Group
Judy Frazier	Administrative Analyst/Specialist, Information Technology Services
Anna Pavin	Interim Associate Vice President, Human Resources
Judy Swanson	Manager, IT User Services
Joann Stuermer	Recruiting and Training Coordinator, Human Resources
Dale Velador	PeopleSoft Security Administrator

March 15, 2010

RECEIVED
UNIVERSITY AUDITOR

MAR 11 2010

THE CALIFORNIA STATE
UNIVERSITY

Mr. Larry Mandel
University Auditor
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4200

Dear Larry:

I am pleased to submit our responses to the recommendations identified in the Information Security Audit Report.

Please let me know if there is further information needed as you review the report.

Very truly yours,



Joanne Coville
Vice President for Finance and Administration

Enc.

cc: Dr. Richard Rush, President; Dr. Michael Berman, Chief Information Officer

JC/pam

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
CHANNEL ISLANDS

Audit Report 09-37

SECURITY GOVERNANCE

SECURITY AUTHORITY AND RESPONSIBILITY

Recommendation 1

We recommend that the campus modify its information security organization to ensure that all security initiatives and committees are aligned to create a cohesive security structure that ensures the campus-approved security plan is implemented in accordance with management intent and oversight. We recommend that one person be assigned overall responsibility for information security initiatives.

Campus Response

We agree. The campus will designate one person to have overall responsibility for information security initiatives, by July 31, 2010.

INFORMATION SECURITY PLAN

Recommendation 2

We recommend that the campus establish a formal risk assessment process to identify and prioritize information security risks, perform a detailed information security risk assessment, and create a formal process for tracking and reporting progress to executive management.

Campus Response

We agree. We are in the process of risk assessment and review and will create a formal process for tracking and reporting progress to executive management at its completion. Will be complete by September 30, 2010.

USE OF EMPLOYEE-OWNED COMPUTERS

Recommendation 3

We recommend that the campus implement measures to ensure that home computers used for campus business purposes are patched and protected from viruses before granting access to network resources.

Campus Response

We agree. The campus will either implement measures to ensure that home computers used for campus business purposes are patched and protected from viruses or we will not allow home computers to be used for campus business purposes. Will be complete by June 30, 2010.

EMPLOYEE SEPARATION

Recommendation 4

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

Campus Response

We agree. The campus will include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data, by June 30, 2010.

SYSTEMS SECURITY AND MONITORING

TECHNICAL VULNERABILITIES

Recommendation 5

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

Campus Response

We agree. The campus will repair all the technical vulnerabilities that were identified and presented in detail during the exit interview, by June 30, 2010.

WEBSITE VULNERABILITY MANAGEMENT

Recommendation 6

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

In addition, we recommend that the campus implement a management process for periodic review of existing web application code to minimize its potential susceptibility to new vulnerabilities.

Campus Response

We agree. The campus has already repaired the website vulnerabilities that were identified and presented in detail. By June 30, 2010, the campus will implement a management process for an annual review of existing web application code.

CONFIGURATION CHANGES

Recommendation 7

We recommend that the campus:

- a. Develop policies and procedures to establish a formal review of system configurations so that management can determine accountability for potentially misconfigured network devices and assign responsibility for identifying and remediating configuration problems.
- b. Incorporate into these change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance with configuration reviews.

Campus Response

We agree. The campus will develop policies and procedures to establish a formal review of system configurations so that management can determine accountability for potentially misconfigured network devices and assign responsibility for identifying and remediating configuration problems. We will incorporate into these change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance with configuration reviews. This new process and procedure will be in place by August 30, 2010.

VULNERABILITY MANAGEMENT

Recommendation 8

We recommend that the campus implement intrusion detection provisions to monitor and respond to potential security events.

Campus Response

We agree. The campus will implement intrusion detection provisions to monitor and respond to potential security events, by June 30, 2010.

PASSWORD STANDARDS

Recommendation 9

We recommend that the campus extend its password policy to all servers and network devices and implement procedures to ensure compliance with the policy.

Campus Response

We agree. The campus will extend its password policy to all servers and network devices and implement procedures to ensure compliance, by June 30, 2010.

GRANTING OF ADMINISTRATIVE ACCESS

Recommendation 10

We recommend that the campus establish a formal process for granting privileged system-level access to accounts and that it develop a method to track, review, and periodically audit this type of access.

Campus Response

We agree. The campus will establish a formal process for granting privileged system-level access to accounts and develop a method to track, review and periodically audit this type of access, by July 31, 2010.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

Recommendation 11

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

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. Identify potential or known vulnerabilities by extending the patch management process to include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the network environment.

Campus Response

We agree. The network device vulnerabilities that were identified and presented have been repaired. The campus will formalize a baseline standard that requires the review of network devices for security vulnerabilities prior to deployment and we will identify potential or known vulnerabilities by extending the patch management process to include the review of existing device configurations on a periodic basis and new configurations prior to deployment into the network, by July 31, 2010.

NETWORK ARCHITECTURE

Recommendation 12

We recommend that the campus review its current network topology and determine the most logical way to separate Internet-accessible devices from other devices within the internal network.

Campus Response

We agree. The campus is reviewing our current network topology and we will determine the most logical way to separate Internet-accessible devices from other devices within the internal network, by June 30, 2010.

REVIEW OF SECURITY EVENT LOGS

Recommendation 13

We recommend that the campus establish a formal regularized process to review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of campus systems. This process could include the use of tools and analytical methods and should define personnel responsibilities, reviewing frequency, and reporting/escalating procedures.

Campus Response

We agree. The campus will establish a formal regularized process to review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of campus systems. The process will include the use of tools and analytical methods and will define personnel responsibilities, reviewing frequency, and reporting/escalating procedures. This will be complete by July 31, 2010.

PROTECTED DATA

SYSTEM BACKUP ENCRYPTION

Recommendation 14

We recommend that the campus encrypt any system backups that contain protected information when stored at off-site locations.

Campus Response

We agree, and this has already been completed. Beginning August 2009, all system backups that are stored at off-site locations are now encrypted.

INCIDENT RESPONSE MANAGEMENT

Recommendation 15

We recommend that the campus:

- a. Implement a method to consistently record all information security-related incidents.
- b. Enhance its reporting process to ensure that the information security officer is notified of all computer security incidents reported to the university police department.

Campus Response

We agree. The campus will implement a method to consistently record all information security-related incidents and make sure that the ISO is notified of all computer security incidents reported to the university police department, by July 31, 2010.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR



BAKERSFIELD

March 29, 2010

CHANNEL ISLANDS

CHICO

MEMORANDUM

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed
Chancellor

A handwritten signature in black ink that reads "Charles B. Reed".

FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 09-37 on *Information Security*,
California State University, Channel Islands

LONG BEACH

LOS ANGELES

In response to your memorandum of March 29, 2010, I accept the response as submitted with the draft final report on *Information Security*, California State University, Channel Islands.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS