

INFORMATION SECURITY
SONOMA STATE UNIVERSITY

Audit Report 08-16
October 10, 2008

Members, Committee on Audit

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

Staff

University Auditor: Larry Mandel
Senior Director: Michelle Schlack
IT Audit Manager: Greg Dove
Senior Auditor: Dominick Owens

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
Policy Issuance, Maintenance, and Approval	8
Payment Card Industry Data Security Standard.....	9
Mobile Computing	10
Record Retention.....	10
Decentralized Computing	11
Technical Vulnerabilities	11
E-mail Systems	13
System Development and Change Management.....	14
Systems Security and Monitoring	15
Password Standards.....	15
Application Control.....	17
Audit and Security Event Logs Management	18
Granting Administrative Access	19
Network Monitoring	19
Routing and Switching Devices.....	20
Network Architecture.....	21
Unauthenticated Access	22
Border Firewall Settings	22
Protected Data.....	23
System Backup Encryption	23
Assessment and Inventory of Protected Information	24
Disposition of Protected Data	24
Incident Response Management	25

APPENDICES

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

ABBREVIATIONS

AD	Active Directory
CSU	California State University
EO	Executive Order
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITWSS	Information Technology Workstation Services and Security
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NASA EPO	National Aeronautics and Space Administration Education and Public Outreach Program
PCI DSS	Payment Card Industry Data Security Standard
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSU	Sonoma State University
VLAN	Virtual Local Area Network

EXECUTIVE SUMMARY

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

We visited the Sonoma State University campus from May 12, 2008, through June 27, 2008, and audited the procedures in effect at that time.

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

In our opinion, the operational and administrative controls of information security in effect as of June 27, 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]

Information security policy issuance and maintenance was not always complete or timely, and the procedures for formal approval of information security policies needed improvement. The campus and auxiliaries had not completed a Payment Card Industry Data Security Standard (PCI DSS) self-assessment questionnaire to determine if its areas accepting credit cards compelled the campus to conduct a PCI DSS compliance summary plan. Lastly, the campus lacked adequate policies and procedures for the security of remote computing and the campus had not completed a record retention action plan consisting of procedures to ensure appropriate and timely disposal of records/information.

DECENTRALIZED COMPUTING [11]

Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the campus IT team and were not held to the same programming standard and code review or security configuration standards. Decentralized departmental e-mail server environments lacked comprehensive policies and procedures and were not always adequately maintained and secured.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [14]

Web application vulnerabilities existed on several websites selected for testing.

SYSTEM SECURITY AND MONITORING [15]

There was no formal password policy and existing password settings did not always ensure adequate security. The campus lacked guidelines for the control of software applications on state purchased machines to ensure that the appropriate use policy was followed. The central IT team had enabled the logging and retention of security events with the use of a syslog server; however, there was no formal policy in place to review these security event logs. The campus lacked a formal process for granting privileged access to accounts and for identifying and monitoring all IT resources on the campus network. 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 adequately secured the campus local area network and wireless network. Border firewall settings were not always properly configured or adequately secured.

PROTECTED DATA [23]

Daily backup copies for systems with protected data were not encrypted when stored locally or when in transit to Humboldt State University for disaster recovery purposes. Although the campus performed an assessment and inventory of protected information, there did not appear to be a formal documented process for classifying and securing its information assets. The campus could not provide evidence documenting the deletion of protected data from campus computers. The investigation of protected data that might exist on lost/stolen computers was inadequate.

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 Sonoma State University (SSU), 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 SSU 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 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

POLICY ISSUANCE, MAINTENANCE, AND APPROVAL

Information security policy issuance and maintenance was not always complete or timely, and the procedures for formal approval of information security policies needed improvement.

We found that:

- ▶ The campus did not have a comprehensive information security policy that was easily accessible to the campus community. Although we found several individual security policies in both formal and draft form, they collectively did not include a specific explanation of standards, security education requirements, details on the prevention of viruses and other malware, compliance with legislative and contract requirements, and references to other documentation, which may support the policy. Additionally, we met with the computer science department and noted that it was unaware of the information security policies posted on the website.
- ▶ Two draft policies (protected data and interim information security incident policy) reviewed had not been formally submitted to the administrative and finance cabinet for policy consideration. This prevented the official distribution of such policies throughout campus and therefore restricted compliance enforcement. In addition, the draft policies lacked accountability as they did not identify the preparer's name, department, and the date in which the policies were drafted.
- ▶ Although campus e-mail systems controls were in place, we noted that the campus did not have a documented policy for the security and management of e-mail systems that would address protection measures regarding malicious software such as computer viruses, spam filtering, and Trojan horses at both the server and desktop levels.

The information security officer stated that this condition was due to the campus involvement in the development of the California State University (CSU) information security policies and standards, for which the campus was also waiting for completion in order to start implementation. He also stated that in the interim, he wrote new and updated policies that he felt were absolutely necessary.

Failure to finalize and communicate campus-wide policy increases the risk of unauthorized exceptions, and could compromise compliance with statutory information security requirements. Such inaction also impacts the ability of the campus to opine on the overall effectiveness of existing security provisions related to such data.

Recommendation 1

We recommend that the campus develop information security policies and procedures for the areas noted without formal policies, finalize and issue policies in draft form, and also develop an action plan for the implementation of the CSU systemwide information security policies and standards.

Campus Response

We agree. Policies will be written for the following areas and submitted for official campus approval:

- ▶ Security training requirements.
- ▶ E-mail security.
- ▶ The prevention of viruses and other malware.

These three policies will be in compliance with legislative and contract requirements. We will submit the current draft policies (i.e., “Protected Data” and “Information Security Incident Policy”) for official campus approval. The campus will also develop an action plan for the implementation of the CSU systemwide information security policies and standards once they become finalized. These will be completed by April 1, 2009.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The campus and auxiliaries had not completed a Payment Card Industry Data Security Standard (PCI DSS) self-assessment questionnaire to determine if its areas accepting credit cards compelled the campus to conduct a PCI DSS compliance summary plan. In addition, responsibility for assessing campus and auxiliary PCI DSS compliance was not defined.

The information security officer stated his belief that the lack of assessment and other required actions could be attributed to uncertainty regarding recent compliance updates to the PCI DSS requirements.

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

Recommendation 2

We recommend that the campus complete the PCI DSS self-assessment questionnaire and define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

Campus Response

We agree. The campus will perform a survey of credit card use at Sonoma State University (SSU), fill out the appropriate PCI DSS questionnaires for the various credit card usage types existing on our campus, and submit the filled out questionnaires to the university’s acquiring financial institution(s). The campus will also establish responsibility for assessing PCI DSS compliance. These will be completed by April 1, 2009.

MOBILE COMPUTING

The campus lacked adequate policies and procedures for the security of remote computing.

We found that there were no documented controls in place for the management of anti-virus and patch updates on remote machines connecting to the internal campus network or for the encryption or backup of data handled by remote users.

The information security officer stated that that this condition was due to the campus waiting for completion of the CSU information security policies and standards in order to start implementation.

Failure to prohibit access to protected data through the use of an employee's personal computer and a lack of security controls for remote users increase the risk that sensitive information could be inadequately secured and increases campus exposure to security breaches.

Recommendation 3

We recommend that the campus document procedures and implement controls to ensure that network security is maintained through remote computing. Such controls for remote computing may include, but not be limited to, requiring the use of virtual private networks, requiring updated anti-virus software and updated security patches, requiring encryption technologies for the use of protected data, and prohibiting the storage of protected data on personal machines.

Campus Response

We agree. The campus will develop mobile computing standards and procedures that are consistent with the CSU security standards. Standards and procedures will be submitted for official campus approval by April 1, 2009.

RECORD RETENTION

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

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

The information security officer stated that archiving within Common Management Systems was currently not supported within the baseline application. He also stated that the CSU chancellor's office was investigating the roll out of a systemwide archiving solution to meet the needs of all the supported applications.

Failure to ensure appropriate and timely disposal of records/information in accordance with legal requirements may result in non-compliance with state and federal laws and regulations and may also result in operational inefficiencies and inconsistent record retention practices across the CSU.

Recommendation 4

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

Campus Response

We agree. We will have an EO 1031 records retention action plan developed by April 1, 2009.

DECENTRALIZED COMPUTING

TECHNICAL VULNERABILITIES

Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the campus information technology (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 the following vulnerabilities (for which specific details were provided to the campus):

Two servers were available through virtual network computing which employed weak access controls, two servers were configured with File Transfer Protocol that authorized world-writable directories and thus permitted unauthorized hosting, one server was a remote hosting wireless access point that allowed possible entry to the internal campus network, three servers were remote hosts with missing operating system fixes for known security issues, two servers were running vulnerable versions of Secure Shell (SSH) authentication software, 15 servers were running vulnerable versions of Remote Desktop Protocol, 22 servers were remote hosts running an outdated common management agent with known security issues, six servers were running vulnerable versions of a retrospect client application, one server was using a version of File Transfer Protocol software that was vulnerable to a glob heap corruption flaw, two servers were remote hosts running a vulnerable version of Apache software that was susceptible to an off-by-one buffer overflow attack, one server was running a vulnerable version of Hypertext Preprocessor with known security issues.

Additionally, deployment of servers in the decentralized computing environment was unmanaged and lacked professional standards and guidance. The decentralized servers were not routinely patched, as a formal patch management process was not in place to govern the implementation of security patches across the campus and ancillary owned assets. Also, there was no baseline security standard for server security or application security, and professional application development standards and methodologies were absent or not adequate.

The information security officer stated that these vulnerabilities were related to servers not under IT control as the management and maintenance of servers and desktops is largely decentralized. He also stated that the campus did not have an efficient way of detecting and mitigating rogue wireless access points, and there was no separate patch for the version of SSH that was running on the end-of-life Cisco Content Services switches. He added that campus server security standards and guidelines were approved in April 2008 and they were not yet implemented by the start of the audit.

Server vulnerabilities increase the risk of a remote attacker 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. Network resources that do not have the latest security patches applied are vulnerable to both external and internal attacks. The lack of formalized processes may lead to an ineffective strategy for mitigating potential vulnerabilities.

Recommendation 5

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. 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.
- b. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.
- c. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the non-IT units with a security baseline standard for securing servers prior to allowing them to become Internet facing.

Campus Response

We agree. The campus will repair the technical vulnerabilities discovered by the KPMG scans.

In addition, the campus will:

- a. Implement a process to review web applications as specified in a new SSU code review standard.
- b. Develop a campus-wide Internet-facing web application development standard to which all developers must comply prior to deploying any web application and submit the web application for official campus approval.

- c. Develop a campus-wide Internet-facing web application development standard to which all developers must comply prior to deploying any Internet-facing web application and submit the web application for official campus approval.
- d. Provide each non-IT department that runs servers with the SSU standards for secure servers.

These will be completed by April 1, 2009.

E-MAIL SYSTEMS

Decentralized departmental e-mail server environments lacked comprehensive policies and procedures and were not always adequately maintained and secured.

We found that:

- ▶ The computer science department e-mail server had a non-spam filtering policy and no monitoring guidelines to limit the possibility of significant damage to the organization's e-mail infrastructure and its users.
- ▶ The computer science department and National Aeronautics and Space Administration Education and Public Outreach Program (NASA EPO) did not have a documented acceptable use policy or a documented security and management of e-mail systems policy.
- ▶ The NASA EPO e-mail servers were not always physically secured. The door to the workspace in which they were housed remained open for climate control purposes at all times.

The information security officer stated that a few computer science faculty members studied spam and did not necessarily want it removed and as a result, spam management was handled at the workstation level. He further stated that the computer science department and NASA EPO did not have an acceptable use policy or e-mail policy because they tended to refer users to the campus policy. The information security officer added that he was unaware that these servers were unsecured.

Lack of consistent documented policies and procedures increases the risk that the various IT services business units may not be performing leading security practices in an effective and consistent manner while IT business units that do not conform to formal/secured processes increase the risk of a breach of protected information.

Recommendation 6

We recommend that the campus:

- a. Implement campus server security standards and guidelines and ensure that relevant e-mail security controls are also addressed by campus-wide policy.

- b. Ensure that decentralized departmental units adhere to campus acceptable use and e-mail policies or have adequately documented their independent policies.
- c. Ensure that all campus servers are provided with adequate physical security.

Campus Response

We agree.

- a. The campus will implement existing SSU server security standards. The campus will write an e-mail security standard, which will be submitted for official campus approval.
- b. We will widely distribute the SSU server security standards, the e-mail security policy and standards, and acceptable use policy — especially to those non-IT departments who run servers.
- c. An information security office staff member will perform a yearly physical survey of the data centers of non-IT departments and report the findings to the information security officer.

These will be completed by April 1, 2009.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

Web application vulnerabilities existed on several websites selected for testing.

Our review of selected websites disclosed the following vulnerabilities (for which specific details were provided to the campus):

One website permitted directory listings of files located on the server, one website listed miscellaneous unrelated files, backups, and unused or obsolete files, one server returned Structured Query Language error messages that could possibly reveal too much information, one website allowed the Autocomplete attribute for user credentials, one website allowed the caching of secured pages, and one website allowed cross-site scripting to bypass access controls.

The information security officer stated that these vulnerabilities may be attributed to development oversights and that this system was still under development and had not been cleaned up in a few areas.

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 7

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

In addition, we recommend that the campus:

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

Campus Response

We agree. The campus will repair the technical web vulnerabilities discovered by the KPMG scans.

- a. SSU will develop a campus-wide application development standard to which all developers must comply prior to deploying an application.
- b. SSU will implement a process to review applications as specified in the new campus code review standard.

These will be completed by April 1, 2009.

SYSTEMS SECURITY AND MONITORING

PASSWORD STANDARDS

There was no formal password policy and existing password settings did not always ensure adequate security.

We found that:

- ▶ There was no formal password policy to govern the enterprise Active Directory (AD) password policy schema.
- ▶ The following AD password parameters were set outside of leading security standards:
 - Minimum Password Length: six characters
 - Password must meet complexity requirements: Disabled
 - Maximum Password Age: 180 days
 - Minimum Password Age: zero days
 - Enforce Password History: two passwords remembered

- ▶ Password controls were not adequate in the PeopleSoft system for those accounts that do not use the centralized authentication system (Lightweight Directory Access Protocol (LDAP)). The following PeopleSoft password controls were set outside of leading security standards:
 - Password Never Expires
 - Minimum Password Length: six characters
 - Number of Special Characters Required: zero
 - Number of Digits Required: zero
 - Password History: zero number of passwords to retain

Also, during our review of the Solar\Enterprise server, we noted a total of 50 user accounts that appeared to have non-expiring passwords.

Leading security practices typically call for AD password policy parameters that include the following: maximum password age of 60-90 days; account lockout threshold of six attempts; and reset account lockout counter of 15 minutes. Also, the AD password policy settings of enforced password history set to two passwords remembered and zero days minimum password age, when combined, could permit a user to quickly recycle two dummy passwords in order to return to their original password, which is not acceptable password policy.

The information security officer stated that the parameters were documented but not implemented and this condition may be attributed to an oversight. He further stated that the non-expiring passwords were both service and test accounts and an accumulation of accounts from the Windows NT era that had not been brought up to current standards.

Insufficient password parameters may compromise the authentication credentials of students, faculty, and administrative user account privileges that are embedded into applications and operating systems; all of which can lead to unauthorized access to network resources and confidential information.

Recommendation 8

We recommend that the campus:

- a. Implement a formal password standard and incorporate it into the existing IT security policy.
- b. Review the current enterprise AD account policy settings and PeopleSoft account settings and develop a threshold that adequately balances security and business enablement across the enterprise environment.
- c. Require all user accounts to have password expirations.

Campus Response

We agree.

- a. We will incorporate a formal password standard into current IT security policy that is consistent with the existing CSU security standard and submit it for official campus approval.
- b. We will implement a formal password standard in AD, LDAP, and PeopleSoft that adequately balances security and business enablement across the enterprise environment.
- c. All end-user account passwords will expire in 90 days.

These will be completed by April 1, 2009.

APPLICATION CONTROL

The campus lacked guidelines for the control of software applications on state purchased machines to ensure that the appropriate use policy was followed.

Application control within certain functional business areas could be administered through central management (i.e., AD); however, the local administrative accounts in other areas could not be held to the same application control standards.

The director of workstation services and security stated that the majority of users with administrative access to their computers were faculty, who believed that it was their right as faculty to have such access and that they were equipped to manage their own computers. He also stated that there was insufficient staffing and resources to provide support to this group at a level that provided a response time that would satisfactorily meet their needs.

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

Recommendation 9

We recommend that the campus further develop application control guidelines to ensure that the campus appropriate use policy is followed by all campus users.

Campus Response

We agree. We will write guidelines requiring IT pre-approval of all software installations for those individuals with administrative access to their computers. This will be completed by January 31, 2009.

AUDIT AND SECURITY EVENT LOGS MANAGEMENT

The central IT team had enabled the logging and retention of security events with the use of a syslog server; however, there was no formal policy in place to review these security event logs.

The information security officer stated that Cisco Security Monitoring, Analysis and Response System provides security monitoring for network and security devices and host applications made by Cisco and other providers. Additionally, he stated that the campus was also waiting for completion of the CSU information security policies and standards, for which the campus would implement.

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

Recommendation 10

We recommend that the campus:

- a. Establish a formal process to regularly document the review and analysis of the security logging data to assist in identifying potential network vulnerabilities and breaches on campus systems. This process may include usage of tools and analytical methods, defining personnel responsibilities, 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 agree.

- a. We will run tools to inspect logs or have a person inspect logs and document the inspection on a daily basis. A formal process will be used to document the review and analysis of logging data.
- b. We will complete the evaluation and planning for an upgraded security logging notification system to replace our current Security Event Correlator software.

These items will be completed by April 1, 2009.

GRANTING ADMINISTRATIVE ACCESS

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

We noted that there was no formal documentation and/or approval for the granting of administrative and service accounts, and as a result, logging and tracking had not been performed.

The information officer stated that the lack of a formal process for the granting of privileged access resulted in the limited documented controls (i.e. logging and tracking).

The lack of a standard process for granting privileges may lead inadequate segregation of duties or the granting of accounts not based on the principle of least privilege.

Recommendation 11

We recommend that campus establish a formal standard for the management of administrative and service accounts taking in 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 agree. SSU will develop a standard for the management of administrative and service accounts consistent with the CSU security standard and submit it for official campus approval. Some areas already have developed methods to provide track, review, and audit access to privileged accounts. The director in each IT department (including Common Management Systems) that controls administrative and service accounts will ensure that a formal process for tracking, reviewing, and auditing access to these types of accounts exists. These will be completed by April 1, 2009.

NETWORK MONITORING

The campus lacked a formal process to identify and monitor all IT resources on the campus network.

The information security officer stated that decentralized servers were not always placed in the campus data center. Additionally, he stated that the campus was also waiting for completion of the CSU information security policies and standards, for which the campus would implement.

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 12

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 agree.

- a. IT will develop a procedure where no static Internet Protocol address gets assigned to a non-IT server until an approval process takes place.
- b. We will employ multiple techniques to begin identifying and monitoring IT assets on the campus network.

These will be completed by April 1, 2009.

ROUTING AND SWITCHING DEVICES

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

Our review of the selected routing and switching devices disclosed that:

- ▶ Two devices were configured with Simple Network Management Protocol (SNMP) version 1, which was unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ One device was enabled with Telnet, which could allow a remote attacker to obtain confidential authentication tokens to permit remote access to the devices in question as user logins, passwords, and commands are transferred across the network in clear text.

The information security officer stated that the network management applications used to monitor the various devices did not all support SNMP version 3, and that the previous version of CiscoWorks required that Telnet be enabled on the virtual tele-typewriter lines even though it did not use that protocol to connect to the device to download the configuration.

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 disable additional network resources.

Recommendation 13

We recommend that the campus:

- a. Disable SNMP version 1 on these network devices. If SNMP is required, version 3 should be configured with authorization and privilege authentication.
- b. Replace Telnet access with SSH or another more secured form of terminal access.

Campus Response

We agree.

- a. We will disable SNMP version 1 and enable SNMP version 3 with authorization and privilege authentication on these network devices identified by the June 25, 2008, KPMG report.
- b. We will replace Telnet on this router identified by the June 25, 2008, KPMG report.

These will be completed by January 30, 2009.

NETWORK ARCHITECTURE

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

The information security officer stated that the campus had successfully relied on the highly segmented nature of the campus network architecture with stringent internal firewall rules to restrict access to campus virtual local area network (VLAN).

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 14

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

Campus Response

We agree. SSU will separate Internet accessible servers from those servers that are accessed only from the local campus. This will be completed by April 1, 2009.

UNAUTHENTICATED ACCESS

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

The campus LAN was available to any machine that was plugged-in, as login credentials (user ID and password) were not required to gain Internet access hosted by the campus. The campus wireless network was also available to any machine within range as login credentials (user ID and password) were not required to gain guest Wi-Fi Internet access hosted by the campus. Although the campus had partitioned the network into several VLANs and limited Wi-Fi network access, the possibility that unauthorized users would have access to local devices and campus resources was present.

The information security officer stated that limited campus resources prevented the implementation of network access control.

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

Recommendation 15

We recommend that the campus strengthen controls to adequately secure the campus LAN and wireless network.

Campus Response

We agree. SSU will strengthen controls for wireless and wired LANs in the following manner:

Wireless LAN. The new Aruba wireless infrastructure will only allow LDAP authentication for known users. Special guest accounts for visitors can be obtained upon request. This will be completed by January 30, 2009.

Wired LAN. All jacks connected to privileged networks (i.e., networks or VLANs) that have potential access to local repositories of protected data) will not be in public areas. This will be completed by April 1, 2009.

BORDER FIREWALL SETTINGS

Border firewall settings were not always properly configured or adequately secured.

Our review of the selected firewall device disclosed that:

- ▶ Firewall device settings supported only SNMP versions 1 and 2c, which could allow an attacker who was able to monitor network traffic to capture device configuration settings, including authentication details.
- ▶ SSH protocol version 1 was supported, which could allow an attacker to capture network traffic and possibly authentication credentials.

The information security officer stated that the campus used SMARTS to receive traps generated by the Cisco PIX firewalls in the event of link up/down, etc. He further stated the campus planned to disable SNMP completely during the next network outage window in three weeks (at the time of our review).

The unencrypted nature of SNMP versions 1 and 2c, could allow an attacker who was able to monitor network traffic to capture device configuration settings, including authentication details.

Recommendation 16

We recommend that the campus:

- a. Disable SNMP on this firewall device.
- b. Configure firewall to support a more secured version of the SSH protocol (i.e., version 2 or later).

Campus Response

We agree.

- a. The SNMP on a firewall, identified by the June 25, 2008, KPMG report, has already been disabled.
- b. The firewall will be upgraded to support SSH version 2 by January 23, 2009.

PROTECTED DATA

SYSTEM BACKUP ENCRYPTION

Daily backup copies for systems with protected data were not encrypted when stored locally or when in transit to Humboldt State University for disaster recovery purposes.

The information security officer stated that limited campus resources prevented the campus from implementing backup encryption.

Inadequate security of daily backups increases the likelihood of inappropriate access to protected data.

Recommendation 17

We recommend that the campus encrypt system backups with protected data when stored and when in transit.

Campus Response

We agree. We will encrypt all tape backups. This will be completed by April 1, 2009.

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

Although the campus performed an assessment and inventory of protected information, there did not appear to be a formal documented process for classifying and securing its information assets.

The information security officer stated that the lack of a formal documented process for the comprehensive assessment or inventory of the protected data residing on campus systems and machines had not yet been formalized.

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 18

We recommend that the campus document a policy or standard that defines responsibility and reporting requirements for performing assessments, as well as overall responsibility for consolidation of campus-wide assessment results.

Campus Response

We agree. The campus will adopt the appropriate portion of the CSU information security standards, which defines who has overall responsibility for consolidation of campus-wide assessment results, and this document will be submitted for official campus approval. This will be completed by April 1, 2009.

DISPOSITION OF PROTECTED DATA

The campus could not provide evidence documenting the deletion of protected data from campus computers.

Using a sample of ten computers that were disposed of from October 2006 to December 2007, the campus was unable to provide any evidence of hard drive wiping.

Although the Information Technology Workstation Services and Security (ITWSS) department recently developed an internal procedure (guidelines for preparing computers for survey) for wiping and logging computing equipment, we noted that there was no campus-wide procedure regarding the hard drive wiping of equipment that did not belong to or go through the ITWSS prior to disposal.

The information security officer stated that computing equipment maintained outside the control of the ITWSS department was not subject to hard drive wiping or the procedures upheld at the ITWSS.

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 19

We recommend that the campus develop and implement a campus-wide policy for the disposal/transfer of IT assets to ensure that hard drive wiping is sufficiently documented and retained.

Campus Response

We agree. A policy and procedure will be implemented where both the transfer of ownership and disposal of all desktops, laptops, and server involve hard drive wiping and logging. This will be completed by April 1, 2009.

INCIDENT RESPONSE MANAGEMENT

The investigation of protected data that might exist on lost/stolen computers was inadequate.

Our review of ten computers reported as lost or stolen from October 2005 to December 2007 disclosed that:

- ▶ In eight instances, there was no evidence on file to show that the first respondents to computer theft investigations inquired about the potential compromise of protected data or the campus efforts to notify affected parties of potential losses.
- ▶ In three instances, the incidents were not investigated/formally reported from four to 12 months after they occurred.

The chief information officer stated that these instances presented themselves and procedures were not addressed because the information security office and the university police department had not collaborated to establish a response protocol in this regard.

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

Recommendation 20

We recommend that the campus document the investigation of all lost/stolen equipment in a timely manner and reiterate the importance of inquiring about the potential loss of protected data when computing equipment is involved.

Campus Response

We agree. A procedure will be devised where all lost or stolen campus-owned IT equipment is investigated and documented in a timely manner. This will be completed by April 1, 2009.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Ruben Armiñana	President
Barry Blackburn	Information Security Officer, Information Technology
Geoff Cirullo	Associate Director, Administrative Information Systems
Letitia Coate	Controller
Peter Flores	Common Management Systems Security Administrator
Laurence Furukawa-Schlereth	Vice President, Administration and Finance and Chief Financial Officer
Mark Harlin	Property Program Coordinator
Kurt Koehle	Director, Internal Operations Analysis and Review
Richard Ludmerer	Senior Director, Risk Management
Roger Mamer	Systems Administrator, Computer Science Department
Robin Marshall	Director, Workstation Services and Security, Information Technology
Ruth McDonnell	Director, Contracts and Procurement, Payables
Brian Orr	Senior Accountant, Financial Services
Sam Scalise	Chief Information Officer
Lou Ann Seaman	Director, Administrative Information Systems
Kathleen Spitzer	Managing Director, Employee Services
Joyce Suzuki	Managing Director, Employee Relations and Compliance Services
Jason Wenrick	Senior Director, Common Management Systems
Deanna Wilson	Managing Director, Payroll and Benefits



1801 East Cotati Avenue
Rohnert Park, CA 94928-3609

OFFICE OF THE CHIEF FINANCIAL OFFICER AND
VICE PRESIDENT FOR ADMINISTRATION AND FINANCE

707.664.2035 • Fax 707.664.2080

November 19, 2008


RECEIVED
UNIVERSITY AUDITOR

NOV 24 2008

THE CALIFORNIA STATE
UNIVERSITY

MEMORANDUM

TO: Larry Mandel
University Auditor
California State University
401 Golden Shore, 4th Floor
Long Beach, California 90802-4200

FROM: Larry Furukawa-Schleith 
Vice-President, Administration and Finance
Chief Financial Officer

SUBJECT: Campus Response to Recommendations, Information Security Audit Report # 08-16

On behalf of President Armiñana, I am submitting the initial campus response to the recommendations of *Audit Report 08-164, Information Security at Sonoma State University*.

The response will also be forwarded to your staff electronically.

We are taking action to implement the recommendations, and will provide documentation to demonstrate completion of corrective actions for each recommendation.

Enclosures

c: President Ruben Armiñana
Eduardo Ochoa, Provost and Vice President for Academic Affairs
Matthew Lopez-Phillips, Acting Vice President for Student Affairs
Dan Condron, Vice President, University Affairs
Letitia Coate, Associate Vice President, Administration and Finance
Samuel Scalise, Senior Director, Information Technology and Chief Information Officer
Jason Wenrick, Senior Director, Common Management Systems (CMS)
Barry Blackburn, Information Security Officer, Information Technology
Kurt Koehle, Director of Internal Operations, Administration and Finance

THE CALIFORNIA STATE UNIVERSITY

INFORMATION SECURITY
SONOMA STATE UNIVERSITY
Audit Report 08-16

SECURITY GOVERNANCE

POLICY ISSUANCE, MAINTENANCE, AND APPROVAL

Recommendation 1

We recommend that the campus develop information security policies and procedures for the areas noted without formal policies, finalize and issue policies in draft form, and also develop an action plan for the implementation of the CSU systemwide information security policies and standards.

Campus Response

We agree. Policies will be written for the following areas and submitted for official campus approval:

- security training requirements
- email security
- the prevention of viruses and other malware

These three policies will be in compliance with legislative and contract requirements.

We will submit the current draft policies (i.e., “Protected Data” and “Information Security Incident Policy”) for official campus approval.

The campus will also develop an action plan for the implementation of the CSU system wide information security policies and standards once they become finalized.

These will be completed by April 1, 2009.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Recommendation 2

We recommend that the campus complete the PCI DSS self-assessment questionnaire and define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

Campus Response

We agree. The campus will perform a survey of credit card use at SSU, fill out the appropriate Payment Card Industry Data Security Standards (PCI DSS) questionnaires for the various credit card usage types existing on our campus, and submit the filled out questionnaires to the university’s

acquiring financial institution(s). The campus will also establish responsibility for assessing PCI DSS compliance. These will be completed by April 1, 2009.

MOBILE COMPUTING

Recommendation 3

We recommend that the campus document procedures and implement controls to ensure that network security is maintained through remote computing. Such controls for remote computing may include, but not be limited to, requiring the use of virtual private networks, requiring updated anti-virus software and updated security patches, requiring encryption technologies for the use of protected data, and prohibiting the storage of protected data on personal machines.

Campus Response

We agree. The campus will develop mobile computing standards and procedures that are consistent with the CSU Security Standards. Standards and procedures will be submitted for official campus approval by April 1, 2009.

RECORD RETENTION

Recommendation 4

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

Campus Response

We agree. We will have an Executive Order 1031 records retention action plan developed by April 1, 2009.

DECENTRALIZED COMPUTING

TECHNICAL VULNERABILITIES

Recommendation 5

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. 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.
- b. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.

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

Campus Response

We agree. The campus will repair the technical vulnerabilities discovered by the KPMG scans.

In addition, the campus will:

- a. Implement a process to review web applications as specified in a new SSU code review standard.
- b. Develop a campus-wide Internet-facing web application development standard to which all developers must comply prior to deploying any web application and submit the web application for official campus approval.
- c. Develop a campus-wide Internet-facing web application development standard to which all developers must comply prior to deploying any Internet-facing web application and submit the web application for official campus approval.
- d. Provide each non-IT department that runs servers with the SSU standards for secure servers.

These will be completed by April 1, 2009.

E-MAIL SYSTEMS

Recommendation 6

We recommend that the campus:

- a. Implement campus server security standards and guidelines and ensure that relevant e-mail security controls are also addressed by campus-wide policy.
- b. Ensure that decentralized departmental units adhere to campus acceptable use and e-mail policies or have adequately documented their independent policies.
- c. Ensure that all campus servers are provided with adequate physical security.

Campus Response

We agree.

- a. The campus will implement existing SSU server security standards. The campus will write an email security standard which will be submitted for official campus approval.
- b. We will widely distribute the SSU server security standards, the email security policy and standards, and acceptable use policy - especially to those non-IT departments who run servers.

- c. An Information Security Office staff member will perform a yearly physical survey of the data centers of non-IT departments and report the findings to the Information Security Officer.

These will be completed by April 1, 2009.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

Recommendation 7

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

In addition, we recommend that the campus:

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

Campus Response

We agree. The campus will repair the technical web vulnerabilities discovered by the KPMG scans.

- a. SSU will develop a campus-wide application development standard to which all developers must comply prior to deploying an application.
- b. SSU will implement a process to review applications as specified in the new campus code review standard.

These will be completed by April 1, 2009.

SYSTEMS SECURITY AND MONITORING

PASSWORD STANDARDS

Recommendation 8

We recommend that the campus:

- a. Implement a formal password standard and incorporate it into the existing IT security policy.
- b. Review the current enterprise AD account policy settings and PeopleSoft account settings and develop a threshold that adequately balances security and business enablement across the enterprise environment.
- c. Require all user accounts to have password expirations.

1/12
1/12

Campus Response

We agree.

- a. We will incorporate a formal password standard into current IT security policy that is consistent with the existing CSU Security Standard and submit it for official campus approval.
- b. We will implement a formal password standard in Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and PeopleSoft that adequately balances security and business enablement across the enterprise environment.
- c. All end-user account passwords will expire in 90 days.

These will be completed by April 1, 2009.

APPLICATION CONTROL

Recommendation 9

We recommend that the campus further develop application control guidelines to ensure that the campus appropriate use policy is followed by all campus users.

Campus Response

We agree. We will write guidelines requiring IT pre-approval of all software installations for those individuals with administrative access to their computers. This will be completed by January 31, 2009.

AUDIT AND SECURITY EVENT LOGS MANAGEMENT

Recommendation 10

We recommend that the campus:

- a. Establish a formal process to regularly document the review and analysis of the security logging data to assist in identifying potential network vulnerabilities and breaches on campus systems. This process may include usage of tools and analytical methods, defining personnel responsibilities, 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 agree.

- a. We will run tools to inspect logs or have a person inspect logs and document the inspection on a daily basis. A formal process will be used to document the review and analysis of logging data.

- b. We will complete the evaluation and planning for an upgraded security logging notification system to replace our current Security Event Correlator software.

We will have these items completed by April 1, 2009.

GRANTING ADMINISTRATIVE ACCESS

Recommendation 11

We recommend that campus establish a formal standard for the management of administrative and service accounts taking in 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 agree.

SSU will develop a standard for the management of administrative and service accounts consistent with the CSU Security Standard and submit it for official campus approval.

Some areas already have developed methods to provide track, review, and audit access to privileged accounts. The director in each IT department (including CMS) that controls administrative and service accounts will ensure that a formal process for tracking, reviewing, and auditing access to these types of accounts exists.

These will be completed by April 1, 2009.

NETWORK MONITORING

Recommendation 12

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 agree.

- a. IT will develop a procedure where no static Internet Protocol (IP) address gets assigned to a non-IT server until an approval process takes place.
- b. We will employ multiple techniques to begin identifying and monitoring IT assets on the campus network.

These will be completed by April 1, 2009.

ROUTING AND SWITCHING DEVICES

Recommendation 13

We recommend that the campus:

- a. Disable SNMP version 1 on these network devices. If SNMP is required, version 3 should be configured with authorization and privilege authentication.
- b. Replace Telnet access with SSH or another more secured form of terminal access.

Campus Response

We agree.

- a. We will disable Simple Network Management Protocol (SNMP) version 1 and enable SNMP version 3 with authorization and privilege authentication on these network devices identified by the June 25, 2008 KPMG report.
- b. We will replace Telnet on this router identified by the June 25, 2008 KPMG report.

These will be completed by January 30, 2009.

NETWORK ARCHITECTURE

Recommendation 14

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

Campus Response

We agree. SSU will separate Internet accessible servers from those servers that are accessed only from the local campus. This will be completed by April 1, 2009.

UNAUTHENTICATED ACCESS

Recommendation 15

We recommend that the campus strengthen controls to adequately secure the campus LAN and wireless network.

Campus Response

We agree. SSU will strengthen controls for wireless and wired Local Area Networks (LANs) in the following manner:

Wireless LAN. The new Aruba wireless infrastructure will only allow LDAP authentication for known users. Special guest accounts for visitors that can be obtained upon request. This will be completed by January 30, 2009.

Wired LAN. All jacks connected to privileged networks (i.e., networks or Virtual Local Area Networks (VLANs) that have potential access to local repositories of protected data) will not be in public areas. This will be completed by April 1, 2009.

BORDER FIREWALL SETTINGS

Recommendation 16

We recommend that the campus:

- a. Disable SNMP on this firewall device.
- b. Configure firewall to support a more secured version of the SSH protocol (i.e. version 2 or later).

Campus Response

We agree.

- a. The Simple Network Management Protocol (SNMP) on a firewall, identified by the June 25, 2008 KPMG report, has already been disabled.
- b. The firewall will be upgraded to support Secure Shell (SSH) version 2 by January 23, 2009.

PROTECTED DATA

SYSTEM BACKUP ENCRYPTION

Recommendation 17

We recommend that the campus encrypt system backups with protected data when stored and when in transit.

Campus Response

We agree. We will encrypt all tape backups. This will be completed by April 1, 2009.

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

Recommendation 18

We recommend that the campus document a policy or standard that defines responsibility and reporting requirements for performing assessments, as well as overall responsibility for consolidation of campus-wide assessment results.

Campus Response

We agree. The campus will adopt the appropriate portion of the CSU Information Security Standards, which defines who has overall responsibility for consolidation of campus-wide assessment results and this document will be submitted for official campus approval. This will be completed by April 1, 2009.

DISPOSITION OF PROTECTED DATA

Recommendation 19

We recommend that the campus develop and implement a campus-wide policy for the disposal/transfer of IT assets to ensure that hard drive wiping is sufficiently documented and retained.

Campus Response

We agree. A policy and procedure will be implemented where both the transfer of ownership and disposal of all desktops, laptops, and server involve hard drive wiping and logging. This will be completed by April 1, 2009.

INCIDENT RESPONSE MANAGEMENT

Recommendation 20

We recommend that the campus document the investigation of all lost/stolen equipment in a timely manner and reiterate the importance of inquiring about the potential loss of protected data when computing equipment is involved.

Campus Response

We agree. A procedure will be devised where all lost or stolen campus-owned IT equipment is investigated and documented in a timely manner. This will be completed by April 1, 2009.



THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

January 22, 2009

CHANNEL ISLANDS

CHICO

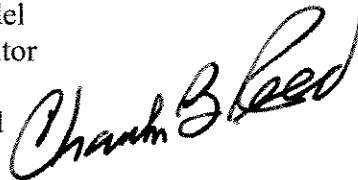
MEMORANDUM

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed
Chancellor


FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 08-16 on *Information Security*,
Sonoma State University

LONG BEACH

LOS ANGELES

In response to your memorandum of January 22, 2009, I accept the response as submitted with the draft final report on *Information Security*, Sonoma State University.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/jt

POMONA

Enclosure

SACRAMENTO

cc: Dr. Ruben Armiñana, President

SAN BERNARDINO

Mr. Laurence Furukawa-Schlereth, Vice President, Administration and
Finance and Chief Financial Officer

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS