

INFORMATION SECURITY
CALIFORNIA STATE POLYTECHNIC UNIVERSITY,
POMONA

Audit Report 08-15
September 26, 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
IT Audit Manager: Greg Dove
Audit Manager: Gary Miller
Senior Auditor: Alec Lu

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

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

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance.....	8
Policy Issuance and Maintenance	8
Payment Card Industry Data Security Standard.....	11
Decentralized Computing	12
System Development and Change Management.....	14
Web Application Development and Maintenance	14
Web Application Vulnerabilities.....	16
Systems Security and Monitoring	17
Vulnerability Management	17
Application Control.....	18
Network Monitoring	18
Audit and Security Event Logs Management	20
Control Over User Access.....	21
Password Standards.....	22
Granting Administrative Access	23
Network Architecture.....	24
Network and Telecommunications Devices.....	24
Protected Data.....	26
Assessment and Inventory of Protected Information	26
Disposition of Protected Data	27

APPENDICES

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

ABBREVIATIONS

CSPUP	California State Polytechnic University, Pomona
CSU	California State University
DoS	Denial of Service
I&IT	Instructional and Information Technology
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
PCI DSS	Payment Card Industry Data Security Standard
SSH	Secure Shell
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 California State Polytechnic University, Pomona campus from May 5, 2008, through June 6, 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 6, 2008, taken as a whole, were not sufficient to meet many of the objectives for a secured computing environment. While much of the campus IT department control environment was satisfactory and provided appropriate safeguards over the critical financial and student systems, the decentralized computing environments that were not under the purview of campus IT require significant improvement and management oversight.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations. Our audit did not examine all aspects of information security, but was designed to assess the controls over management, increase awareness, and recommend implementation for significant security topics that are prevalent in the California State University computing environment.

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

SECURITY GOVERNANCE [8]

The campus had not finalized and communicated information security policies, standards, and guidelines, and the current information security program was not sufficient to address current campus business practices and operations. In addition, the campus and auxiliaries had not completed a Payment Card Industry Data Security Standard compliance summary plan to define their applicable vendor level and respective contractual requirements.

DECENTRALIZED COMPUTING [12]

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

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [14]

Application development and change management was not adequate to ensure accountability for authorized deployment of web development projects. In addition, vulnerabilities existed on one web application selected for testing.

SYSTEM SECURITY AND MONITORING [17]

The campus lacked a standard process to detect vulnerabilities or exploits related to security of servers and desktops connected to the campus network. The campus also lacked guidelines for the control of software applications on state purchased machines to ensure that the appropriate use policy was being followed, and a formal process to identify and monitor all IT resources on the campus network, whether owned and managed by central I&IT or ancillary IT sites. Log management guidelines for managing, securing, and reviewing audit and security event logs of operating systems, servers, and applications were not consistent across the campus, and the review of such logs was not always adequate. In addition, the administration of user accounts and the processes for requesting, approving, and monitoring user access to systems and applications were not adequately controlled, there was no formal policy for assigning passwords to administrative and service accounts, and the campus lacked a formal process for granting privileged access to accounts. Further, Internet accessible devices were located within the same segments as internal resources. Also, the management of network and telecommunication devices attached to the campus network required improvement.

PROTECTED DATA [26]

The campus lacked procedures for and had not conducted a comprehensive assessment or inventory of the protected data residing on campus systems and machines. In addition, procedures to ensure that all sensitive information on computers was properly deleted prior to disposition required improvement.

INTRODUCTION

BACKGROUND

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

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

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

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

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

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

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

At California State Polytechnic University, Pomona (CSPUP), the office of IT 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 systems 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 CSPUP 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 AND MAINTENANCE

The campus had not finalized and communicated information security policies, standards, and guidelines, and the current information security program was not sufficient to address current campus business practices and operations.

We found that:

- ▶ The campus had not updated its current information security program to reflect changes in the campus' business practices and operations. The current information security program was drafted in 2003 to meet certain specific compliance requirements, but it had not been updated to address other more recent compliance requirements.
- ▶ The campus had not ensured that individual departments conducted annual data security reviews in accordance with the information security program.
- ▶ Campus information security policies, standards, and guidelines were not always complete; few were finalized; and many existed only in draft form. The lack of finalization had prevented the official distribution of such policies throughout campus and restricted compliance enforcement.
- ▶ The campus had not developed an e-mail policy, standards, or guidelines to address the security, management, ownership, and record retention of the e-mail systems, which were identified as the primary communications medium on campus.

The information security officer stated that the campus had delayed updating the campus information security program due to awaiting the deployment of California State University (CSU) information security policies and standards. He further stated that the campus had instead focused on the drafting and development of campus information security standards covering data classification, desktop and server security, and information security incident management, which were under review at the start of the audit by the campus information security technology and security governance councils. He added that the campus had not developed a specific policy to address the use of e-mail, relying instead on the appropriate use policy to guide end users use of campus technology resources.

Security practices that fail to ensure campus-wide policy and compliance increase the risk of unauthorized exceptions and could compromise compliance with statutory information security requirements thus, impacting the campus' ability to opine on the overall effectiveness of existing security provisions related to such data.

Recommendation 1

We recommend that the campus:

- a. Evaluate and update its current information security program to reflect current business practices and operations.
- b. Ensure that individual departments conduct annual data security reviews in accordance with the information security program requirements.
- c. Finalize and communicate information security policies, standards, and guidelines throughout the campus.
- d. Evaluate its e-mail requirements and develop an e-mail policy to address the security, management, ownership, and record retention of the e-mail systems.

Campus Response

We concur.

- a. The information security program was evaluated in 2007 using the International Organization for Standardization (ISO) 27001/ISO 27002 information security standard. The findings of that assessment were incorporated in the campus information security strategic plan. The information security program will be updated to reflect the information security strategic plan and current campus operations.

Timeline: April 2009

- b. Individual departments will be required to conduct annual assessments in accordance with the updated information security program.

Timeline: April 2009

- c. Information security policies, standards, and guidelines will be communicated to the campus in accordance with standard campus procedures.

1. Guideline on the management of administrative and service accounts will be provided.

Timeline: February 2009

2. Vulnerability assessment process will be in place.

Timeline: January 2009

3. An updated information and classification and handling standard will be disseminated.

Timeline: January 2009

4. Additional guidelines regarding appropriate use will be disseminated.

Timeline: January 2009

5. Security event logging and reporting requirements will be added to the campus security standards.

Timeline: February 2009

6. The user account management guidelines will be disseminated campus-wide.

Timeline: February 2009

7. Process to manage the deployment of servers onto the campus network.

Timeline: March 2009

8. Web application security vulnerability guideline.

Timeline: March 2009

9. Web application development standard.

Timeline: April 2009

10. Information security program.

Timeline: April 2009

11. Campus e-mail guidelines.

Timeline: April 2009

- d. E-mail security and retention requirements will be evaluated and a guideline will be developed covering e-mail security, ownership, and record retention.

Timeline: April 2009

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

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

We found that:

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

The information security officer stated that the campus and auxiliaries had been waiting for additional guidance from the chancellor's office regarding the scope and applicability of the PCI requirement to the individual campuses.

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:

- a. Conduct a PCI assessment to determine its applicable vendor level and respective PCI requirements.
- b. Define and document responsibility for assessing campus and auxiliary PCI DSS compliance.
- c. Complete all PCI requirements including annual risk assessments and quarterly network scans by an approved vendor, if required.

Campus Response

We concur.

- a. The campus and its auxiliaries will complete a PCI assessment.

Timeline: January 2009

- b. Roles and responsibilities regarding PCI compliance will be documented in the updated campus information security program.

Timeline: March 2009

- c. The campus will complete all PCI requirements.

Timeline: March 2009

DECENTRALIZED COMPUTING

Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the central instructional and information technology (I&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 running legacy operating systems no longer supported by the vendor, one server was susceptible to directory traversal, five servers allowed Hypertext Preprocessor attacks, two servers were running deprecated software vulnerable to denial of service (DoS) attack, one server was using a version of file transfer protocol software that was vulnerable to a glob heap corruption flaw, two servers were running vulnerable versions of server authentication software (SSH), one server was vulnerable to heap overflow, 14 servers were running vulnerable versions of remote desktop protocol, one server was running a software version vulnerable to privilege escalation, one server was vulnerable to domain name service zone transfers, one server for virtual network computing did not require authentication, one server was running a software version vulnerable to DoS, two servers were running hypertext forms which would pass in input password over plain text, 17 servers allowed connectivity through Telecommunication Network, a highly unsecured authentication process, and one server was running remote shell service, which is not ciphered and could allow sensitive data to be sniffed.

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 decentralized servers not under I&IT control which were either unpatched, in the process of being retired, or in the process of upgrading to newer software. He added that campus server security standards and guidelines were approved in April of 2008, but were not implemented by the start of the audit.

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

Recommendation 3

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

In addition, we recommend that the campus:

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

Campus Response

We concur. The campus has repaired all the technical vulnerabilities presented to the campus and will provide documentation.

Timeline: December 2008

- a. Comprehensive patch management processes were documented in the desktop and server security standards and guidelines. The IT Governance Council approved the desktop and server security standards and guidelines in April 2008.

Timeline: December 2008

- b. The campus security standards have been provided to ancillary IT units and are available on demand via the campus information security group in Blackboard.

Timeline: December 2008

- c. The server security guidelines will require a review of security vulnerabilities prior to deployment into the campus production environment. This requirement will be implemented after the vulnerability assessment tools are deployed campus-wide.

Timeline: January 2009

- d. A web application development security vulnerability guideline will be developed that includes a checklist of potential and common security vulnerabilities to review. Before developers deploy an application into a production environment, they will be asked to review the security vulnerability checklist.

Timeline: April 2009

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

WEB APPLICATION DEVELOPMENT AND MAINTENANCE

Application development and change management was not adequate to ensure accountability for authorized deployment of web development projects.

Application development and change management processes were generally informal in the areas outside of central I&IT. Within certain areas in central I&IT the application development process was also deficient. Our review of central I&IT and various other divisions on the campus that performed some degree of web application development disclosed that:

- ▶ Formal approval was not required for projects put into production.
- ▶ Security criteria for testing procedures were not documented.
- ▶ User acceptance procedures were not documented.
- ▶ Programmers had unlimited access to the source code.
- ▶ Version control of the source code was not possible.

Additionally, the campus had not developed a formal process to manage outsourced web application development. We noted that various divisions and auxiliaries contracted with third-party developers for web applications independent of central I&IT. Although this process was acceptable for the actual development of the application, final acceptance was not conducted in conjunction with central I&IT to ensure that web applications meet minimum web application security standards as established by the campus.

The information security officer stated that web application development at CSPUP is largely decentralized. He added that while central I&IT was responsible for the development and implementation of campus-wide applications such as the campus identity management system, other divisions had developed division specific applications. He further stated that processes regarding web application development, as a result, had evolved independently with no coordination by central I&IT.

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

Recommendation 4

We recommend that the campus:

- a. Develop a formal approval process for all web application development that uses campus resources.
- b. Develop formal documentation of security criteria for testing procedures, including but not limited to, input and output validation tests.
- c. Develop formal documentation for user acceptance and deployment.
- d. Ensure that the web application source code is protected by limiting access to those who need it.
- e. Obtain version control software to ensure that inadvertent source code revisions can be rolled back to previous versions for applications developed across campus.
- f. Ensure that web applications developed by third-party developers are formally reviewed and approved by central I&IT prior to final acceptance and implementation to ensure that web applications meet minimum web application security standards as established by the campus.

Campus Response

We concur.

- a. The campus will develop guidelines and standards for web application development that campus IT departments will be asked to follow.

Timeline: April 2009

- b. The web application security vulnerability guideline will cover secure development practices and how to test for vulnerabilities.

Timeline: April 2009

- c. The web application development standard will cover user acceptance and deployment practices.

Timeline: April 2009

- d. The web application development standard will encourage business users and developers to limit access to production code to those who need it.

Timeline: April 2009

- e. Large-scale web application developers will be encouraged to use source code control software during software development.

Timeline: April 2009

- f. The web application development standard will require that web applications developed by third parties be reviewed for adherence to minimum campus application security standards and tested for security vulnerabilities prior to deployment into production.

Timeline: April 2009

WEB APPLICATION VULNERABILITIES

Vulnerabilities existed on one web application selected for testing.

The web application allowed the auto complete attribute for user credentials, the caching of secured pages, and phishing through Uniform Resource Locator redirection. In addition, it was running deprecated software with multiple known vulnerabilities, allowed cross-site scripting to bypass access controls, and allowed hypertext transfer protocol injection to deliver attacks.

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

Web application vulnerabilities increase the risk of exploitation by a remote attacker 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 5

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 formalize a security standard that requires detailed testing of web applications for security vulnerabilities prior to deployment.

Campus Response

We concur. The campus has repaired all website vulnerabilities identified in the campus audit and documentation will be provided in December. Websites were rescanned using the campus vulnerability scanning tools to confirm that items identified in the audit were fixed. The campus web

application development standard and guideline will address the need to test for security vulnerabilities prior to application deployment.

Timeline: December 2008

SYSTEMS SECURITY AND MONITORING

VULNERABILITY MANAGEMENT

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

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

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 forestall the spread of vulnerabilities and exploits from one campus virtual local area network (VLAN) to the next. He added that the campus had not had a campus-wide exploit in at least four years and that other security initiatives had taken a higher priority over the development of a standard process to detect vulnerabilities.

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

Recommendation 6

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

Campus Response

We concur. The campus is developing a vulnerability assessment process in parallel with the rollout of the campus vulnerability assessment tools.

Timeline: January 2009

APPLICATION CONTROL

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

The information security officer stated that the campus had largely relied on the appropriate use policy to guide end users in the use of campus technology resources. He added that desktop standards and guidelines were approved in February 2008, but were not implemented by the start of the audit.

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 7

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 concur. The campus will develop additional guidelines to ensure that all campus users follow the campus' appropriate use policy.

Timeline: January 2009

NETWORK MONITORING

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

We noted that:

- ▶ Any user on the network had the ability to place a server on the campus network without central I&IT permission. Servers were generally restricted to a certain segment on the campus network via VLAN; however, a compromised server could lead to further campus exposure if the VLAN was improperly configured or if the server contained sensitive information.
- ▶ Web servers that were externally viewable from a public domain were not actively monitored or controlled by central I&IT. Central I&IT had the ability to identify potential web servers based on the submission of a request for a fixed IP address, but it did not actively monitor whether the configuration on the web server was adequate to prevent the server from being compromised.

The information security officer stated that the management and maintenance of servers on the campus network was largely decentralized and users were encouraged to place their servers in the

central I&IT campus data center. He further stated that the campus server security standards and guidelines were approved in April of 2008, but were not implemented by the start of the audit.

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. Such inability increases the risk that an attacker could inject malicious code or viruses into the network or compromise confidential information.

Recommendation 8

We recommend that the campus:

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

Campus Response

We concur.

- a. The campus will develop a formal process to manage the deployment of servers onto the campus network.

Timeline: March 2009

- b. All campus owned IT assets connected to the campus network will be identified and monitored based on the assets' security risk profiles.

Timelines:

1. September 2009 – The identification and campus-wide monitoring process will begin in January, but given the number of assets to monitor, it will not be complete until September 2009.
2. March 2009 – Servers with Level 1 (confidential) protected information.
3. June 2009 – Other assets with Level 1 (confidential) and Level 2 (internal use only) protected information.

AUDIT AND SECURITY EVENT LOGS MANAGEMENT

Log management guidelines for managing, securing, and reviewing audit and security event logs of operating systems, servers, and applications were not consistent across the campus, and the review of such logs was not always adequate.

We found that:

- ▶ Every custodian of operating systems, servers, and applications was responsible for determining and implementing best practices for log management with no general oversight or direction from central I&IT.
- ▶ Although the I&IT server team had enabled the logging of security events for the Windows and UNIX servers selected for testing, there was no periodic review of these logs.

The information security officer stated that management and maintenance of audit and security event logs of servers and desktops was largely decentralized, and while the server security standards and guidelines were approved in April of 2008, they were not implemented by the start of the audit. He added that although a log review had been performed by the I&IT server team, this informal process had not been documented due to a lack of resources and the large number of logs created.

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

Recommendation 9

We recommend that the campus:

- a. Establish a formal process to regularly document the review and analysis of the audit and 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 concur.

- a. The campus will expand the campus security standards to address security event logging and reporting requirements.

Timeline: February 2009

- b. The campus will assess the need for centralized information/event monitoring with regards to security events.

Timeline: March 2009

CONTROL OVER USER ACCESS

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

Our review of 15 user accounts on three selected systems disclosed that:

- ▶ Three general user accounts were shared among various users.
- ▶ Two user accounts were active even though the employees had been terminated more than a year ago. Also, the process for removing user accounts from terminated employees was not always documented.
- ▶ Four user accounts lacked confidentiality agreements on file, a requirement for users with access to protected data.
- ▶ Periodic management review for user access within all systems and applications containing protected data was not performed and documented.

The information security officer stated that the campus had drafted user account management guidelines, but the campus had not universally implemented these guidelines by the start of the audit.

Failure to properly administer user accounts and adequately control access to systems and applications increases the risk of inappropriate access to sensitive data and non-compliance with information security policies by employees.

Recommendation 10

We recommend that the campus:

- a. Eliminate general user accounts and assign unique user accounts with defined accountability.

- b. Formalize a process for managing and removing user accounts for terminated employees.
- c. Ensure that user confidentiality agreements are completed and retained for those users with access to protected data.
- d. Conduct and document periodic reviews of user access to systems containing protected data, at least on an annual basis.

Campus Response

We concur.

- a. The campus has removed the general user accounts identified in the applications assessed in the audit, and documentation will be provided in December 2008.

Timeline: December 2008

- b. The campus has drafted guidelines regarding user account management. The guidelines include processes for removing user accounts for terminated employees. The guidelines will be disseminated campus-wide.

Timeline: February 2009

- c. The user account management guideline and the campus information classification and handling standard requires that users with access to protected data have a signed copy of the employee confidentiality statement on file with the human resources department before access is granted to a system with protected data.

Timeline: April 2009

- d. The campus will review on an annual basis user account management guidelines compliance.

Timeline: April 2009

PASSWORD STANDARDS

The campus lacked a formal policy for assigning passwords to administrative and service accounts.

We noted that that the I&IT server team utilized an informal process to deploy account policies that govern user authentication to critical network resources.

The information security officer stated that the informal server password policy was in the process of being formalized when the audit was conducted.

Lack of a formal policy for the assignment of passwords to administrative and service accounts may lead to compromised account privileges and further compromising campus network resources and confidential information.

Recommendation 11

We recommend that the campus establish a formal password policy for assigning passwords to administrative and service accounts.

Campus Response

We concur. In the interim, before the CSU Systemwide Information Security Policy is created and released, the campus will draft guidelines regarding the management of administrative and service accounts and documentation. The new guidelines will include a section on the assignment of passwords. Upon release of the CSU Systemwide Information Security Policy, the campus will modify the campus guidelines (if necessary) and adopt the password standard of the systemwide policy.

Timeline: February 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 security officer stated that an informal process of granting privileged access was in the process of being formalized when the audit was conducted.

Lack of a formal process for granting privileged access may lead to inadequate segregation of duties or the granting of access not based on the principle of least privilege.

Recommendation 12

We recommend that campus establish a formal process for the management of administrative and service accounts taking into account the criteria for individuals who should have access, roles, and responsibilities for these resources and develop a method to track, review, and periodically audit this type of privileged access.

Campus Response

We concur. The campus will draft guidelines regarding the management of administrative and service accounts. The new guidelines will include a section on who should be granted access, roles and responsibilities, and a process to assess compliance on a periodic basis.

Timeline: February 2009

NETWORK ARCHITECTURE

Internet accessible devices were located within the same segments as internal resources. Normally, these Internet accessible devices are segmented into a demilitarized zone such that if these devices are compromised, there is 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 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 13

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

Campus Response

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

Timeline: April 2009

NETWORK AND TELECOMMUNICATIONS DEVICES

The management of network and telecommunication devices attached to the campus network required improvement.

We noted the following:

- ▶ The campus had not performed an assessment to determine if approved modems were properly secured, as the security of these devices was unknown.

- ▶ The campus had not documented a periodic assessment of rogue wireless access points and its disposition. Campus policy requires I&IT to monitor and disconnect access points upon discovery; however, periodic assessments had not been documented to demonstrate that unmanaged access points were addressed in a timely manner.

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 forestall the spread of vulnerabilities and exploits from wireless access points to the campus VLAN. He further stated that the campus had not had a campus-wide exploit in at least four years and other security initiatives had taken a higher priority over the documentation of unmanaged wireless access points and the assessment of modems.

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

Recommendation 14

We recommend that campus:

- a. Conduct a security review of the existing modem inventory to ensure that minimum security standards are maintained.
- b. Document the periodic assessment of unmanaged wireless access points to ensure that unmanaged access points are addressed in a timely manner.

Campus Response

We concur.

- a. The campus completed a security risk assessment of modems on campus to ensure that they did not pose a threat to the integrity of the network and documentation will be provided in December 2008.

Timeline: December 2008

- b. The campus has documented the process in place to address the risk of unmanaged wireless access points and documentation will be provided in December 2008.

Timeline: December 2008

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

The campus lacked procedures for and had not conducted a comprehensive assessment or inventory of the protected data residing on campus systems and machines. Such an assessment would reference applications, servers/systems, databases, storage locations, protected data types, approximations for number of protected data files, existing security controls, interfaces with other systems, custodians of record, technical security officers, and individuals permitted access.

The information security officer stated that while the campus information classification and handling standards were approved in April 2008, the campus had not started the confidential data inventory project by the start of the audit. He further stated that a pilot of the data identification and inventory process was completed in the student affairs division in 2007.

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 15

We recommend that the campus:

- a. Conduct an assessment of the current inventory and security of protected information.
- b. 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 concur.

- a. The campus will complete an assessment of Level 1(confidential), Level 2 (internal use only), and Level 3 (public) protected information, accordingly.

Timelines:

1. April 2009 – Level 1 (confidential).
2. July 2009 – Level 2 (internal use only).
3. October 2009 – Level 3 (public).

- b. Assessment responsibilities will be added to the roles and responsibility section of the information and classification and handling standard.

Timeline: January 2009

DISPOSITION OF PROTECTED DATA

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

The campus could not provide evidence documenting the deletion of protected data from campus computers. The campus policy stated that all computers and laptops should be wiped prior to disposition, but divisions were not required to document that such procedures had been performed nor were there any controls in place to ensure that such procedures had been performed.

The information security officer stated that changes had not been made to the campus property survey form in which a technician would have indicated that a hard drive had been wiped prior to being surveyed.

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 16

We recommend that the campus update its campus property survey forms to ensure that hard drive wiping is sufficiently documented and retained.

Campus Response

We concur. The campus has updated its campus property form to ensure that hard drive wiping is documented and will provide documentation in December 2008.

Timeline: December 2008

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
J. Michael Ortiz	President
Al Arboleda	Information Security Officer, Instructional and Information Technology (I&IT)
Edwin Barnes, III	Vice President, Administrative Affairs and Chief Financial Officer
Debra Brum	Vice President, I&IT
Curtis Clark	Director, I&IT Web Development
Benson Dang	Information Technology Consultant, College of Business Administration
Gabriel Kuri	Senior Network Engineer, I&IT Systems
Darwin Labordo	Associate Vice President, Finance and Administrative Affairs
Richard Leonard	Computer Resource Specialist, College of Letters, Arts and Social Sciences
Joe Matsumoto	Director, I&IT Systems
Billy McCowan	Systems Administrator, College of Business Administration
Kevin Morningstar	Executive Director, Student Affairs Information and Technology Service
Son Pham	Senior Systems Analyst, College of Engineering
Gary Pierce	Information Security Specialist, I&IT
Ernesto Rodriguez	Senior Information Technology Consultant, Academic Resources
Lisa Rotunni	Director, Academic Resources
Randy Townsend	Management Information Systems Manager, Foundation
Joice Xiong	Director of Internal Audit, Administrative Affairs
Glendy Yeh	Executive Director of Information Systems, Administrative Affairs