

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**FULLERTON**

**Audit Report 08-14**  
**August 21, 2008**

---

**Members, Committee on Audit**

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

---

**Staff**

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

---

**BOARD OF TRUSTEES**  
**THE CALIFORNIA STATE UNIVERSITY**

---

## CONTENTS

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

---

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance.....	8
Security Authority and Responsibility .....	8
Policy Issuance and Approval.....	9
Payment Card Industry Data Security Standard.....	10
Decentralized Computing .....	11
Policies and Procedures .....	11
Server Environments.....	12
Technical Vulnerabilities .....	13
System Development and Change Management.....	15
Configuration Changes .....	15
Web Application Development and Maintenance .....	16
Systems Security and Monitoring .....	17
Control Over User Access.....	17
E-mail Systems .....	18
Password Standards.....	19
Review of Security Event Logs .....	20
Protected Data.....	22
Assessment and Inventory of Protected Information .....	22
Use of Employee Owned Computers .....	23
Disposition of Protected Data .....	24
Incident Response Management .....	24

## **APPENDICES**

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

---

## **ABBREVIATIONS**

AD	Active Directory
CITO	Chief Information Technology Officer
CSU	California State University
CSUF	California State University, Fullerton
IEC	International Electrotechnical Commission
IMAP	Internet Message Access Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITS	Information Technology Services
PCI DSS	Payment Card Industry Data Security Standard
POP	Post Office Protocol
SAM	State Administrative Manual
SSL	Secure Sockets Layer

---

## EXECUTIVE SUMMARY

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

We visited the California State University, Fullerton (CSUF) campus from March 3, 2008, through April 18, 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 April 18, 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 formally recognized the information security office and its respective authority on campus. Accordingly, the campus lacked a detailed information security action plan. In addition, the campus had not finalized and communicated information security policies. Also, the campus and auxiliaries had not completed a Payment Card Industry Data Security Standard (PCI DSS) compliance summary plan to define their applicable vendor level and respective contractual requirements. Specifically, 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, responsibility for assessing campus and auxiliary PCI DSS compliance was not defined, and quarterly network scans were not conducted by an approved scanning vendor.

### **DECENTRALIZED COMPUTING [11]**

Information security policies and procedures were neither comprehensive nor applicable to all campus units. In addition, decentralized departmental server environments that contained protected data were not always adequately secured, user accounts were not properly utilized or maintained, and patch management was not comprehensive. Also, technical vulnerabilities existed on a variety of decentralized ancillary systems throughout the campus. These systems were not maintained by the information technology services team and were not held to the same programming standard and code review or security configuration standards.

### **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [15]**

The campus lacked policies and procedures that defined a formal review process for configuration changes to firewalls, switches, routers, and servers/operating systems. In addition, changes to the campus assets were not formally initiated, documented and approved prior to production deployment, periodic configuration reviews were not formalized, and change management was not adequate to ensure accountability for authorized deployment of web development projects.

### **SYSTEM SECURITY AND MONITORING [17]**

The process for monitoring user access to systems and applications was not adequately controlled. In addition, e-mail access and the e-mail transmission of protected data were not always encrypted. Also, the campus had not documented a formal password policy and existing password settings did not always ensure adequate security. Lastly, the review of security event logs was not adequate.

### **PROTECTED DATA [22]**

A periodic inventory and assessment of protected information was not routinely performed because campus requirements for a periodic assessment were not defined. In addition, the campus lacked a policy or standard that restricted the use of employee-owned computers for university business purposes, documentation of hard drive wiping was not available to evidence that any existence of protected data was properly deleted from ten machines that were recently disposed of or redeployed to different users on campus, and campus procedures for the investigation of protected data that might exist on lost/stolen computers were inadequate.

---

## INTRODUCTION

### **BACKGROUND**

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

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

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

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

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

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

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

At California State University, Fullerton (CSUF) 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 CSUF 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. In instances wherein it was necessary to review annualized data, calendar year 2007 or fiscal year 2006/07 was the primary period reviewed except when it was beneficial to see trends for multiple years.

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

### SECURITY AUTHORITY AND RESPONSIBILITY

The campus had not formally recognized the information security office and its respective authority on campus. Accordingly, the campus lacked a detailed information security action plan.

We found that:

- ▶ In March 2004, the campus issued Presidential Directive 13 – *Information Security*, which delegated authority to the vice president of administration and finance to oversee information security policy and coordinate information security efforts across the university. In January 2007, this responsibility was delegated to the chief information technology officer (CITO) who created the information security office and assigned administrative responsibilities to the information security officer. This revised delegation and the commensurate elevation of information security, as a critical responsibility of all campus management, was not formally communicated within the campus to facilitate effective compliance efforts.
- ▶ The elevation of information security as a recognized critical responsibility of all campus management had not been effectively communicated by the use of an information security action plan listing prioritized objectives.

The CITO stated that the campus had intended to accomplish both of these tasks but had encountered some delays because of the information security office transition.

The lack of official recognition and authority of the information security office and the absence of an information security action plan limit the ability to direct a comprehensive system of information security management. Such limitations increase campus exposure to security breaches and the risk of inappropriate access to data and could compromise compliance with statutory information security requirements.

#### **Recommendation 1**

We recommend that the campus:

- a. Revise Presidential Directive 13 to formally recognize the information security office and its respective authority on campus.
- b. Develop and communicate a detailed information security action plan for distribution throughout the campus.

### **Campus Response**

We concur.

- a. The campus has revised Presidential Directive 13 to formally recognize the information security office and its respective authority on campus. The revision was posted on the campus website on September 1, 2008.
- b. The campus has developed a detailed information security action plan for distribution throughout the campus. It will be reviewed by the information security steering committee by the end of October 2008. The subsequent outcome will be posted on the information security website and sent to the chancellor's office.

### **POLICY ISSUANCE AND APPROVAL**

The campus had not finalized and communicated information security policies.

We found that campus information security policies were not always complete, few were finalized, and many were pending formal approval by the campus' academic senate board. The lack of finalization/board action had prevented the official distribution of such policies throughout campus and restricted compliance enforcement. The following policies/procedures were only available in draft form:

- ▶ Information Security Policy
- ▶ Information Security Roles and Responsibilities
- ▶ Information Security Risk Assessment and Controls
- ▶ Information Classification
- ▶ Information Security Controls and Standards
- ▶ Information Security Incident Response Protocol
- ▶ Electronic Mail Policy
- ▶ Access Control Policy

The CITO stated that the reason the policies had not been finalized was due to the campus awaiting direction from the chancellor's office for the issuance of systemwide information security policies.

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 protected data.

### **Recommendation 2**

We recommend that the campus finalize and communicate information security policies.

### **Campus Response**

We concur. The campus will finalize and communicate information security policies by the end of November 2008, subsequent to the information security steering committee meetings.

### **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.
- ▶ Quarterly network scans were not conducted by an approved scanning vendor as required for compliance.

The CITO stated that the campus was aware of PCI DSS standards but was unsure of the campus' applicable vendor level and specific requirements. He further stated that the campus was waiting for some definitive direction from the chancellor's office to assist them in their required assessments.

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 3**

We recommend that the campus:

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

### **Campus Response**

We concur.

- a. The campus will conduct a PCI assessment to determine their applicable vendor level and respective PCI requirements by the end of November 2008.
- b. The information security office will define and document responsibility for assessing campus and auxiliary PCI DSS compliance by the end of November 2008, following approval of the information security steering committee.
- c. The information security office will complete all PCI requirements including annual risk assessments and quarterly network scans by an approved vendor by the end of February 2009.

## **DECENTRALIZED COMPUTING**

### **POLICIES AND PROCEDURES**

Information security policies and procedures were neither comprehensive nor applicable to all campus units.

We noted that the information technology services (ITS) teams were decentralized and independent with each individual team following different processes for the following activities:

- ▶ Change management (operating systems, applications, firewall, routers, and switches).
- ▶ Configuration management.
- ▶ Periodic review of system and device configuration.
- ▶ Review of logs and security events.
- ▶ Security baselines and hardening procedures.
- ▶ Access control/password policies.

The CITO stated that the campus had not considered it a necessity to standardize all ITS processes and that he did not have operational authority over the decentralized units.

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

### **Recommendation 4**

We recommend that the campus create a unified set of IT policies and procedures so that ITS and ancillary IT teams can leverage existing synergies and execute more streamlined IT operations processes. These standardized policies and procedures should include, at a minimum, processes for

configuration management, change management, patch management, log management, and system security management.

### **Campus Response**

We concur. The campus will create a unified set of IT procedures and processes so that ITS and ancillary IT teams can leverage existing synergies and execute more streamlined IT operations processes. These standardized policies and procedures will include overarching processes for configuration management, change management, patch management, log management, and system security management. These procedures and processes will be distributed widely across campus by the end of November 2008.

## **SERVER ENVIRONMENTS**

Decentralized departmental server environments that contained protected data were not always adequately secured, user accounts were not properly utilized or maintained, and patch management was not comprehensive.

We found that:

- ▶ Departmental servers on the campus network were not always in compliance with CSU and campus policy for the encryption of protected data. Specifically, protected information such as social security numbers, credit card numbers, and other personal information was identified in unencrypted formats when performing scans of the servers.
- ▶ Local departmental user accounts (not campus active directory (AD) accounts) were improperly utilized and maintained as user IDs were being shared by multiple employees and not deleted for terminated employees.
- ▶ Patch management was completed on campus for those computers under the purview of ITS, but not for those outside of their control. Therefore, ITS could not ensure that the most current virus definitions and software patches were installed on those machines (PCs, laptops, and servers) that resided behind an internal firewall.

The CITO stated that this condition was due to the campus having several decentralized server environments but lacking centralized policies for ensuring network integrity.

Failure to properly encrypt protected data increases the risk of compromising such data in the event of a security breach, while the failure to enforce the use of individual user IDs compromises the ability to localize accountability for system transactions. Failure to provide a reliable process of desktop software patch management, including updated anti-virus definitions, increases the risk of compromise to campus systems, fraudulent or unauthorized activities, and virus threats.

### **Recommendation 5**

We recommend that the campus:

- a. Issue a memorandum/guidance assigning responsibility to all decentralized departments for proper encryption controls, security of their systems, and patch management.
- b. Enforce the use of no shared user IDs and delete user accounts for terminated employees.
- c. Develop a process for monitoring compliance with security and patch management for those machines residing behind internal firewalls, which are outside of ITS control.

### **Campus Response**

We concur.

- a. The chief information security officer will issue a memorandum/guidance assigning responsibility to all decentralized departments for proper encryption controls, security of their systems, and patch management by the end of October 2008.
- b. The campus will enforce the use of no shared user IDs and delete user accounts for terminated employees by the end of November 2008.
- c. The campus has developed a process for monitoring compliance with security and patch management for those machines residing behind internal firewalls, which are outside of ITS control. This system will be deployed by the end of October 2008.

## **TECHNICAL VULNERABILITIES**

Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the ITS 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):

One server was susceptible to Structured Query Language injection, one server to Directory Traversal, six servers allowed Hypertext Preprocessor attacks, one server was using a version of file transfer software that allowed multiple known vulnerabilities, eight servers were running vulnerable versions of server authentication software (SSH), one server did not prevent listing of its directory contents, five servers allowed connectivity through Telnet, a highly unsecured authentication process, and one server was configured to provide error conditions (Stack Trace) to potential attackers which could provide the intruder with additional information on exploits.

Additionally, deployment of servers in the decentralized computing environment was unmanaged and lacked professional standards and guidance. The decentralized servers were not routinely patched, there was no baseline security standard for server security or application security, and professional application development standards and methodologies were absent or not adequate.

The CITO stated that the lack of centralized policies and procedures had permitted the majority of these vulnerabilities to propagate in the decentralized computing environment.

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 6**

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 ancillary IT units with a security baseline standard for securing servers prior to allowing them to become Internet facing.

### **Campus Response**

We concur. The campus will repair all of the technical vulnerabilities that were identified and presented in detail effective December 2008.

- a. The campus has implemented 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 by the end of November 2008.
- b. The campus has formalized a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This will be reviewed by the information

security steering committee and communicated broadly to technical areas by the end of November 2008.

- c. The campus has developed a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application and it will be in place by the end of November 2008.
- d. IT will provide all the ancillary IT units with a security baseline standard for securing servers prior to allowing them to become Internet facing by the end of November 2008.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

### **CONFIGURATION CHANGES**

The campus lacked policies and procedures that defined a formal review process for configuration changes to the following assets:

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

We noted that changes to these assets were not formally initiated, documented, and approved prior to production deployment. Specifically, we found that ITS had an informal process for requesting, testing, and approving changes including patch, Microsoft, and application updates, hardware changes, and regular maintenance. We also noted that periodic reviews of these assets were informally occurring at regular intervals as part of ITS operational responsibilities; however, this informal process was not adequate to ensure that these network devices adhere to the latest configuration standards and updates.

The CITO stated that the campus had not recognized the need for a formal, documented process.

The lack of a formal policy for documenting configuration changes decreases accountability on changes made to mission critical assets, prevents detection of unauthorized changes to the production environment, and increases the risk of unsupported or unapproved custom configuration changes to the production environment. The lack of periodic review of system and device configuration increases the risk of having inconsistent and deprecated standards, which may permit malicious activity to go undetected.

### **Recommendation 7**

We recommend that the campus:

- a. Develop formal change management policies and procedures that would assist in providing a framework and standard for any system and configuration changes. Such policies should include, but not be limited to, requirements to document all configuration changes made to network devices and servers in the production environment, if there is a business and/or security need to do so, and the types of documentation such as change request forms, approvals, and notifications to develop an audit trail for each change.
- b. Incorporate into these formal change management policies a formal process for the periodic and documented review of system configurations that will assist management with identifying potentially misconfigured network devices. Such periodic review of system and device configurations might occur whenever any configuration changes are made to these assets.

### **Campus Response**

We concur. IT has developed procedures to implement a formal change management process.

- a. The campus will develop formal change management processes and procedures that will assist in providing a framework and standard for any system and configuration changes. Such processes will include requirements to document all configuration changes made to network devices and servers in the production environment, if there is a business and/or security need to do so, and the types of documentation such as change request forms, approvals, and notifications to develop an audit trail for each change. This will be in place by the end of November 2008.
- b. The campus will incorporate into these formal change management procedures a formal process for the periodic and documented review of system configurations that will assist management with identifying potentially misconfigured network devices. Periodic review of system and device configurations may occur whenever any configuration changes are made to these assets. This will be put in place with the change management system by the end of November 2008.

## **WEB APPLICATION DEVELOPMENT AND MAINTENANCE**

Change management was not adequate to ensure accountability for authorized deployment of web development projects.

The campus utilized change management checklists that outlined specific review check points for use by the web developers, database administrators, and web service administrators. However, these checklists were not always signed, dated, and retained. In addition, the process did not prevent programmers from directly modifying the production code without prior authorization.

The CITO stated that while the campus had set procedures for change management, they had neglected to document this process.

Failure to adequately document and retain authorization for the deployment of web development projects increases the risk of unauthorized changes and minimizes the accountability of changes.

**Recommendation 8**

We recommend that the campus properly document and retain the change management checklists and implement controls to prevent unauthorized changes.

**Campus Response**

We concur. The campus will document and retain the change management checklists and implement controls to prevent unauthorized changes. These will take the form of updating already existing checklists and procedures by the end of October 2008.

**SYSTEMS SECURITY AND MONITORING**

**CONTROL OVER USER ACCESS**

The process monitoring user access to systems and applications was not adequately controlled.

Campus management had not implemented any periodic review of user access within all systems and applications containing protected data.

The Common Management Systems project director stated that the periodic review of user access had been done informally in some cases and upon system upgrades in other cases and the process was not documented.

Failure to periodically review user access to systems containing protected data increases the risk of inappropriate access.

**Recommendation 9**

We recommend that the campus conduct and document periodic reviews of user access to systems containing protected data, at least on an annual basis.

**Campus Response**

We concur. The campus will conduct and document periodic reviews of user access to systems containing protected data, at least on an annual basis. As part of this process, the information security office has been designated the responsibility for revising the systems access and approval process. These changes and periodic reviews will be effective by the end of November 2008.

## **E-MAIL SYSTEMS**

E-mail access and the e-mail transmission of protected data were not always encrypted.

We noted that:

- ▶ The Outlook web access was not adequately secured via Secure Socket Layer (SSL) encryption.
- ▶ The outward (off-campus) transmission of Exchange e-mail was not encrypted and the campus lacked software tools to encrypt files containing protected data.
- ▶ The campus lacked documented policies that restricted employees from sending protected data via e-mail.
- ▶ Authentication to the Exchange e-mail servers through the web (squirrel mail) was not adequately secured as user login via Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) did not require some form of encryption such as SSL or Transport Layer Security.

The CITO stated that the unsecured access to webmail was a result of some recent configuration changes that were not properly reset to secure SSL. He stated that the non-encryption of outward transmission of Exchange mail was due to the costs associated with implementing encryption technologies. He further stated that the POP/IMAP condition was a known vulnerability that was permitted to exist in order to provide students with access to their e-mail from mobile devices.

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

### **Recommendation 10**

We recommend that the campus:

- a. Implement SSL encryption for the authentication/login to webmail.
- b. Develop and communicate a policy that restricts employees from sending protected data via e-mail and requires the encryption of protected data when such data must be sent via e-mail.
- c. Consider the use of encrypted authentication via the implementation of secure POP (POPs) and secure IMAP (IMAPs) and the elimination of POP and IMAP.

### **Campus Response**

We concur.

- a. The campus has implemented SSL for authentication and login to the campus Exchange web interface.
- b. The campus has developed and communicated a policy that addresses the issue of employees sending protected data via e-mail and requires the encryption of protected data when such data must be sent via e-mail in the *Cal State Fullerton Guidelines for Securing Electronic Protected Data*.
- c. The campus will consider the use of encrypted authentication via the implementation of secure POP (POPs) and secure IMAP (IMAPs) and the elimination of POP and IMAP as mobile technologies allow. A review of these services is ongoing and will next be addressed by the end of November 2008.

### **PASSWORD STANDARDS**

The campus had not documented a formal password policy and existing password settings did not always ensure adequate security.

The California State University, Fullerton (CSUF) server team uses an informal process to deploy account policies that govern user authentication to Microsoft Windows 2000/2003 servers and network resources. The CSUF server team references the National Security Agency's standard as a guideline to establish basic password policy criteria. However, we found that the following AD password parameters were set outside leading security standards as follows:

- ▶ Maximum password age: 306
- ▶ Account lockout threshold: 30 invalid logon attempts
- ▶ Reset account lockout counter after: 5 minutes

We also noted that 349 of 10,800 accounts had non-expiring passwords on a primary domain controller.

The CITO stated that the campus had not recognized the need for a formal, documented password policy. He further stated that the password age was set to 306 days due to accommodations for the academic calendar and the other settings were not considered as unsecured by the campus. The CITO also stated that the administrator accounts were purposely assigned non-expiring passwords for functional purposes; however, the non-administrator accounts with non-expiring passwords were present due to oversight.

Lack of a documented password policy increases the risk that password parameters within campus systems will be insufficient and inconsistent, while insufficient password parameters increase the risk of unauthorized access to network resources and confidential information.

### **Recommendation 11**

We recommend that the campus:

- a. Document the existing password parameters and formally incorporate this into existing IT security policy.
- b. Review the current enterprise AD account policy 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 concur.

- a. The campus will document the existing password parameters and formally incorporate this into the existing IT security policy/plan by the end of November 2008, following approval of the information security steering committee.
- b. The campus has reviewed the current enterprise AD account policy settings and developed a threshold that adequately balances security and business enablement across the enterprise environment. This will continue to be examined as enterprise applications and services are brought online. A review of these services is ongoing and will next be addressed by the end of November 2008.
- c. The campus has completed the process of requiring that all account passwords, other than system accounts, expire the passwords consistent with emerging CSU and industry standards.

### **REVIEW OF SECURITY EVENT LOGS**

The review of security event logs was not adequate.

We found that:

- ▶ The ITS server team had enabled the logging of security events for the in-scope Windows and UNIX servers. However, there was no periodic review of these logs as they were only stored for 16 hours due to memory and storage limitations. In addition, back-up, which would permit subsequent review, was not in place.
- ▶ The ITS network team informally reviewed security logs, reports, and e-mails that were received from configuration management tools that monitor their devices. However, there was no formal process or procedure in place to review these logs.

The CITO stated that resource constraints had limited the amount of time that personnel could spend manually reviewing logs and that the purchase of an automated tool for centralized security and event logging was also hindered by resource constraints.

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

### **Recommendation 12**

We recommend that the campus:

- a. Establish a formal process to regularly review and analyze the security logging data to assist in identifying potential network vulnerabilities and breaches on campus systems. This process may include usage of tools and analytical methods, defining personnel responsibilities, frequency, and reporting/escalating processes.
- b. Enhance storage limitations to record a reasonable period of time for which security logs will be retained and backed-up in order to permit subsequent review.
- c. 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 establish a formal process to regularly review and analyze the security logging data to assist in identifying potential network vulnerabilities and breaches on campus systems. This process will include usage of tools and analytical methods, defining personnel responsibilities, frequency, and reporting/escalating processes. This will be incorporated into the existing IT security policy/plan by the end of November 2008, following approval of the information security steering committee.
- b. Campus will enhance storage limitations to record a reasonable period of time for which security logs will be retained and backed-up in order to permit subsequent review by the end of November 2008.
- c. The information security office, working with the IT procedures and process workgroup, will consider the implementation of centralized security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification. Recommendations for proceeding on an implementation will be completed by the end of November 2008.

## PROTECTED DATA

### ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

A periodic inventory and assessment of protected information was not routinely performed.

We found that:

- ▶ Campus assessment of the protected information security inventory (by division) was not current; it was last conducted in September 2004 and significant changes had not been reassessed. The prior assessment referenced outdated 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 campus lacked a definitive policy or standard for the coordination of such protected information security inventory, including divisional reporting responsibilities and overall responsibility for consolidation of assessment results.
- ▶ The campus had not performed an assessment to determine if approved modems were properly secured. The total inventory of 1,622 analog phone lines included 163 approved modem lines for which the security was unknown by the campus information security office.

The CITO stated that the protected information security inventory had not been reassessed and the security of the modem lines had not been reviewed because of the administrative transitioning of information security responsibilities from the vice president of administration and finance to the CITO in January 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 13**

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 divisional assessments, as well as overall responsibility for consolidation of campus-wide assessment results.
- c. Conduct a security review of the existing modem inventory to ensure that minimum security standards are maintained.

### **Campus Response**

We concur.

- a. The campus has completed an assessment of the current inventory and security of protected information. Results have transmitted to technical system administrators for remediation and re-review. The campus will be restricting access to these systems using administrative virtual local area networks. The campus will conduct periodic reviews (one/yr) to ensure compliance with existing CSU and campus policy.
- b. As a component of the detailed security action plan, the campus will document a standard that defines responsibility and reporting requirements for performing divisional assessments, as well as overall responsibility for consolidation of campus-wide assessment results. The detailed action plan will be reviewed by the information security steering committee by the end of October 2008.
- c. The campus will conduct a security review of the existing modem inventory to ensure that minimum security standards are maintained. The review will be completed by the end of October 2008.

### **USE OF EMPLOYEE OWNED COMPUTERS**

The campus lacked a policy or standard that restricted the use of employee-owned computers for university business purposes.

The CITO stated that the lack of a policy which specifically prohibited the use of employee-owned computers for university business was an oversight, but added that the campus had communicated the security risks of storing protected data in unencrypted form to employees during mandatory personal computer/laptop training.

Failure to prohibit access to protected data through the use of an employee's personal computer increases the risk that sensitive information could be inadequately secured.

### **Recommendation 14**

We recommend that the campus create a policy restricting the use of employee-owned computers for university business purposes.

### **Campus Response**

We concur. The campus has developed a guideline for home use of privately owned computers and university protected data.

## 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 recently disposed of or redeployed to different users, the campus was unable to provide any evidence of hard drive wiping.

The CSUF Desktop Computing Policy, *Disposal or Transfer of Information Technology Assets*, states that for each drive wiped, sufficient documentation should be retained to verify that destruction of drive content has taken place, using a prescribed sanitation procedure as detailed previously. The campus information security office recommends that a simple logbook be maintained for such task (including date, asset tag, last owner, and disposition). This destruction log should be retained for two years.

The information security officer stated that the campus had a process for wiping all computers when disposed or redeployed but had not required that hard drive wiping be documented.

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.

**Prior to the end of our fieldwork, the campus developed a policy (noted above) for the disposal/transfer of IT assets, which required that hard drive wiping be sufficiently documented and retained.**

### Recommendation 15

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

### Campus Response

We concur. The campus has implemented the procedure for the disposal/transfer of IT assets to ensure that hard drive wiping is sufficiently documented and retained. This process has been amended to include logging for each incident. This amended procedure will be put in place by the end of September 2008.

## INCIDENT RESPONSE MANAGEMENT

Campus procedures for the investigation of protected data that might exist on lost/stolen computers were inadequate.

The procedures only required verbal confirmation from the custodian of the computer as to whether unencrypted protected data was resident. Our review of four computers reported as stolen from

October 2006 to February 2008 disclosed that documentation was not available to evidence the performance of proper investigation procedures and certification by the custodian that protected data was not compromised (including definitions and specifics of protected data).

The CITO stated that the campus had a procedure for investigating whether protected data existed on lost/stolen machines; however, the procedure did not require documentation of such investigation.

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

**Prior to the end of our fieldwork, the campus developed an employee loss-theft checklist that included evidence by sign-off of investigation procedures completed by campus personnel as well as certification by the custodian for the existence of protected data, and which was required to be completed for all lost/stolen computers.**

#### **Recommendation 16**

We recommend that the campus implement the use of the employee loss-theft checklist to ensure that the investigation and certification of protected data is sufficiently documented and retained.

#### **Campus Response**

We concur. The campus has implemented the use of the employee loss-theft checklist to ensure that the investigation and certification of protected data is sufficiently documented and retained. This will be put in place by the end of September 2008.

---

## APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Milton A. Gordon	President
Kerry Boyer	Information Security Officer
Pat Carroll	Executive Assistant to the President
Dale Coddington	Security Architect
Amir Dabirian	Chief Information Technology Officer (CITO) and Chief Information Security Officer
Willie Hagan	Vice President, Administration and Finance
Bahram Hatefi	Director of Internal Audit
Rommel Hidalgo	Information Technology (IT) Projects Coordinator
Denise Johnson	Director of Human Resource Services: Operations
Kenara Ly	Director of Internet Technologies and IT Server Administration
Chris Manriquez	Director of Desktop Computing and Common Management Systems Project Director
Mike Marcinkevicz	Director of Network Management
Pat Nelson	Information Security Office Administrator
Willie Peng	Lead Network Analyst
Sandra Sobel	Executive Assistant to the CITO