

INFORMATION SECURITY
SAN DIEGO STATE UNIVERSITY

Audit Report 08-18
January 15, 2009

Members, Committee on Audit

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

Staff

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

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary..... 1

Introduction 3

 Background..... 3

 Purpose 4

 Scope and Methodology 6

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance 8

 Security Authority and Responsibility 8

 Payment Card Industry Data Security Standard 8

 Record Retention 9

 Information Security Awareness Training 10

 Employee Separation..... 10

Decentralized Computing..... 11

 Server Environments 11

 Technical Vulnerabilities 12

System Development and Change Management 13

 Web Application Development and Maintenance..... 13

 Web Application Vulnerabilities..... 14

Systems Security and Monitoring 15

 Configuration Changes..... 15

 Granting of Administrative Access 16

 Server Log Management 17

 Routing and Switching Devices 17

Protected Data 19

APPENDICES

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

ABBREVIATIONS

CSU	California State University
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITSO	Information Technology Security Office
PCI DSS	Payment Card Industry Data Security Standard
SDSU	San Diego State University
SNMP	Simple Network Management Protocol
Telnet	Telecommunication 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 San Diego State University campus from July 14, 2008, through August 28, 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 August 28, 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 information technology security office had not formally assessed campus adherence to its information security plan, and the campus and auxiliaries had not completed a Payment Card Industry Data Security Standard compliance summary plan. In addition, the campus had not completed a record retention action plan, the campus did not provide information security awareness training to employees hired prior to January 2006 and contractors that had access to protected information, and employee separation documentation did not include a reminder to the separating party of their ongoing legal responsibility for maintaining the security of protected data.

DECENTRALIZED COMPUTING [11]

The campus adopted a formal information security plan in December 2007; however, decentralized departmental IT managers had not implemented the information security plan to ensure compliance throughout the server environments for log management, patch management, and password standards. In addition, technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the campus IT team and were not held to the same programming standard and code review or security configuration standards.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [13]

The change management system lacked a formal software development process to ensure that adequate controls were in place for systems containing protected information, and web application vulnerabilities existed on the websites selected for testing.

SYSTEM SECURITY AND MONITORING [15]

The campus lacked policies and procedures that defined a formal review process for configuration changes to certain assets. Further, the campus also lacked a formal process for granting privileged access to accounts and for the review of server logs. Additionally, routing and switching devices were not always properly configured or adequately secured.

PROTECTED DATA [19]

Campus reporting and investigation of protected data that might exist on lost/stolen computers was inadequate.

INTRODUCTION

BACKGROUND

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

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

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

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

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

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

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

At San Diego State University, the information technology security office is responsible for establishing information security policies, procedures, an information security plan, serving as a central point of contact, and providing technical security support and network security services. However, a significant level of technology decentralization exists and the overall responsibility for the management of many campus systems resides with the departmental IT managers, who are independent of the campus IT department.

PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration of information security and to determine the adequacy of controls over the related processes to evaluate adherence to an industry-accepted standard, ISO 17799/27002, *Code of Practice for Information Security Management*, and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the overall audit objective, specific goals included determining whether:

- ▶ Certain essential administrative and managerial internal controls are in place, including delegations of authority and responsibility, formation of oversight committees, executive-level reporting, and documented policies and procedures.
- ▶ A management framework is established to initiate and control the implementation of information security within the organization and management direction and support for information security is communicated in accordance with business requirements and relevant laws and regulations.
- ▶ All assets are accounted for and have a nominated owner/custodian who is granted responsibility for maintenance and control to achieve and maintain appropriate protection of organizational assets and

information is appropriately classified to indicate the need, priorities, and expected degree of protection when handling the information.

- ▶ Security responsibilities are addressed prior to employment so that users are aware of information security threats and concerns, are equipped to support organizational security policy in the course of their normal work, and responsibilities are in place to ensure user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed.
- ▶ Responsibilities and procedures for the management of information processing and service delivery are defined and technical security controls are integrated within systems and networks.
- ▶ Access rights to networks, systems, applications, business processes, and data are controlled based on business and security requirements by means of user identification and authentication.
- ▶ Formal event reporting and escalation procedures are in place for information security events and weaknesses, and communication is accomplished in a consistent and effective manner allowing timely corrective action to be taken.
- ▶ The design, operation, use, and management of information systems are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.
- ▶ Web application development and change management processes and procedures are adequate to ensure that application security and accessibility is considered during the design phase, that testing includes protection against known vulnerabilities, and that the production servers are adequately protected.
- ▶ E-mail systems are properly configured and managed so that vulnerabilities are not allowed into the network, incidents are properly escalated, campus usage and retention guidelines are followed, and e-mail addresses are maintained in a central location to facilitate campus-wide communications.
- ▶ The operational security of selected operating systems is adequate to prevent the exploitation of vulnerabilities on the internal network by individuals who gain access to it from dial-in connections, the Internet, and hosts on the internal network.
- ▶ The Internet firewall system is sufficient to identify and thwart attacks from the external Internet and filter unwanted network traffic.
- ▶ Selected routing and switching devices are properly managed and configured to effectively provide the designated network security or traffic controls.
- ▶ Systems connected to the Internet make publicly available any information that may provide enticement to penetrate the Internet gateway.

- ▶ Web application vulnerabilities exist that provide the potential for an unauthorized party to subvert controls and gain access to critical and proprietary information, use resources inappropriately, interrupt business, or commit fraud.

SCOPE AND METHODOLOGY

The proposed scope of the audit, as presented in Attachment B, Audit Agenda Item 2 of the January 22-23, 2008, meeting of the Committee on Audit, stated that information security would include a review of the systems and managerial/technical measures for ongoing evaluation of data/information collected; identifying confidential, private, or sensitive information; authorizing access; securing information; detecting security breaches; and security incident reporting and response. Information security includes the activities/measures undertaken to protect the confidentiality, integrity, and access/availability of information including measures to limit collection of information, control access to data and assure that individuals with access to data do not utilize the data for unauthorized purposes, encrypt data in storage and transmission, and implement physical and logical security measures for all data repositories. Potential impacts include inappropriate disclosures of information; identity theft; adverse publicity; excessive costs; inability to achieve institutional objectives and goals; and increased exposure to enforcement actions by regulatory agencies.

In addition to the interviews and inquiry procedures affecting the operation and support of the network devices reviewed by the Office of the University Auditor, we also contracted with KPMG to perform a technical security assessment that included running diagnostic software designed to identify improper configuration of selected systems, servers, and network devices. The purpose of the technical security assessment was to determine the effectiveness of technology and security controls governing the confidentiality, integrity, and availability of selected campus assets. The assessment contained an internal component (within the campus network) and an external component (via the Internet) while encompassing a review of the security standards and processes that govern the San Diego State University campus. Specifically, this configuration testing included assessment of the following technologies:

- ▶ Selected operating system platforms.
- ▶ Border firewall settings.
- ▶ Selected routing and switching devices.
- ▶ Internet footprint analysis.
- ▶ Website vulnerability assessment.

Our study and evaluation were conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the internal administrative, compliance, and operational/technical controls over the management of information security. Specifically, we reviewed and tested:

- ▶ Information security policies and procedures.
- ▶ Information security organizational structure and management framework.
- ▶ Information asset management accountability and classification.
- ▶ Human resources security responsibilities.
- ▶ Administrative and technical security procedures, information processing, and service delivery.
- ▶ Access controls over networks, systems, applications, business processes, and data.
- ▶ Incident response, escalation, and reporting procedures.
- ▶ Compliance with relevant statutory, regulatory, and contractual security requirements.
- ▶ Web application security and applicable change management procedures.
- ▶ E-mail systems management and configuration.
- ▶ Operational security of selected operating system platforms.
- ▶ Security configurations of border firewall settings.
- ▶ Security configurations of selected routing and switching devices.
- ▶ Internet footprints of systems connected to the Internet.
- ▶ Website vulnerabilities stemming from exposures in the server's operating system, server administration practices, or flaws in the web 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 information technology security office (ITSO) had not formally assessed campus adherence to its information security plan.

Although the campus had a formal information security plan that defined programmatic compliance, we noted that compliance with the plan had not been assessed throughout the campus community.

The information security officer stated that the campus plan was adopted in 2007 and an assessment was scheduled later in 2008 to allow departments time to meet compliance.

Failure to assess campus compliance with the information security plan weakens the ITSO's ability to determine campus compliance with established policy and impacts the ability of the campus to opine on the overall effectiveness of existing security provisions related to protected data.

Recommendation 1

We recommend that the campus require the ITSO to routinely assess campus compliance to the information security plan.

Campus Response

We concur. The ITSO has scheduled assessments with each campus information technology (IT) department. Assessments will be completed by May 29, 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.
- ▶ Quarterly network scans were not conducted by an approved scanning vendor as required for compliance.

The information security officer stated that the campus completed an assessment in 2006 and trained on a new standard in 2007. She further stated that a campus assessment was scheduled to begin later this fiscal year.

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, and assign responsibility for ensuring that annual compliance is achieved.
- b. Complete all PCI requirements including annual risk assessments and quarterly network scans by an approved vendor, if required.

Campus Response

We concur. The university will provide a PCI assessment action plan by June 30, 2009. It will include the planned strategy, status of completion, and milestones to satisfy all PCI requirements including annual risk assessments and quarterly network scans.

RECORD RETENTION

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

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

The information security officer stated that the campus was in the rollout phase of its information security plan and record retention was an element of the implementation phase.

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

Recommendation 3

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

Campus Response

We concur. The university will prepare a record retention action plan by July 29, 2009.

INFORMATION SECURITY AWARENESS TRAINING

The campus did not provide information security awareness training to employees hired prior to January 2006 and contractors that had access to protected information.

The information security officer stated that the campus was waiting for completion of the systemwide information security training program that was being developed by the chancellor's office.

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

Recommendation 4

We recommend that the campus develop an action plan for ensuring that all employees and contractors that have access to protected information receive information security awareness training.

Campus Response

We concur. The university will implement the CSU security awareness training by May 1, 2009.

EMPLOYEE SEPARATION

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

The information security officer stated that this condition resulted because it was planned for inclusion later in the information security plan.

Failure to notify separating employees of ongoing legal responsibility to maintain the security of protected data increases the risk of non-compliance with statutory information security requirements for any remaining access to, or unauthorized custody of, protected data that may be available to terminated employees.

Recommendation 5

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

Campus Response

We concur. The university will revise the electronic manager clearance checklist to include a reminder to separating employees. The checklist will be revised by April 30, 2009.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

The campus adopted a formal information security plan in December 2007; however, decentralized departmental IT managers had not implemented the information security plan to ensure compliance throughout the server environments for log management, patch management, and password standards.

We found that:

- ▶ The information security plan addressed log management standards for managing, securing, and reviewing audit logs and security event logs; however, formal log management procedures were not documented throughout the decentralized areas.
- ▶ The information security plan addressed patch management guidelines; however, the campus IT departments reviewed had not documented a formal patch management plan to govern the implementation of security patches. Additionally, there was no formal patch management process to govern the implementation of security patches across the San Diego State University (SDSU) campus. Accordingly, there was no assurance that all campus systems were deploying the latest security patches to its systems.
- ▶ The information security plan addressed password parameters; however, various departments reviewed did not always comply with the standards.
- ▶ Several Internet-facing web servers were not securely configured and there was no formal configuration guideline for web servers.

The information security officer stated that the campus was in the process of implementing an information security plan that required compliance by all departments. She further stated that the campus original patch management solution became obsolete with the release of Windows XP.

Failure to ensure that the information security plan is effectively implemented throughout the campus community weakens the campus security posture and increases the risk of network, systems, or data compromise or loss of availability or integrity. Inadequate guidelines for the 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, which could lead to confidential information being breached and not reported. Network and system resources that do not have the latest security patches applied are vulnerable to both external and internal attacks. Insufficient password parameters can lead to unauthorized access to network resources and confidential information, while unsecure web servers could allow attackers to gain entry into SDSU's network and could lead to the exposure of confidential information.

Recommendation 6

We recommend that the campus ensure that departmental IT managers implement all aspects of the SDSU information security plan including the areas that were identified during the audit.

Campus Response

We concur. Departmental IT managers will develop an implementation plan, by June 30, 2009, for all aspects of the information security plan identified during the audit.

TECHNICAL VULNERABILITIES

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

Our external testing of selected servers disclosed a total of 132 vulnerabilities on a multitude of servers for which specific details were provided to the campus.

The technology security officer stated that the campus was in the process of implementing the campus IT security plan as well as McAfee Foundstone to do vulnerability scanning of critical and border exposed systems.

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 7

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 ensure that departmental IT managers:

- a. Implement the campus patch management standard on all servers and network devices. This process would include the review of existing code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.
- b. Formalize a security review of critical applications or those systems containing protected data for security vulnerabilities prior to deployment.
- c. Implement an application development methodology to which all developers must comply prior to deploying any Internet-facing application.
- d. Comply with the security baseline standard for securing servers prior to allowing them to become Internet facing.

Campus Response

We concur. In addition to repairing all technical vulnerabilities identified:

- a. Departmental IT managers will develop an implementation plan for patch management compliance by June 30, 2009.
- b. Departmental IT managers, with applications containing protected level 1 data, will develop a security review process to detect vulnerabilities by June 30, 2009.
- c. Departmental IT managers, with Internet-facing proprietary applications, will develop a software development process by June 30, 2009.
- d. Departmental IT managers, with servers containing protected level 1 data, will develop a security review process to detect vulnerabilities by June 30, 2009.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

WEB APPLICATION DEVELOPMENT AND MAINTENANCE

The change management system lacked a formal software development process to ensure that adequate controls were in place for systems containing protected information.

The information security officer stated that the campus was in the process of implementing an information security plan that required compliance by all departments, including compliance with the campus standard for a requirements analysis for software development.

The lack of a formal process for software development increases the risk of unapproved software development and unknown security concerns.

Recommendation 8

We recommend that the campus ensure that departmental IT managers implement a formal software development process for critical applications or those systems containing protected data.

Campus Response

We concur. Departmental IT managers, with critical applications or those systems containing protected level 1 data, will develop a software development process by June 30, 2009.

WEB APPLICATION VULNERABILITIES

Web application vulnerabilities existed on the websites selected for testing.

Our review of two selected websites disclosed certain vulnerabilities for which specific details were provided to the campus. Specifically, both websites allowed Structured Query Language error messages that could possibly reveal too much information, cross-site scripting to bypass access controls, and trace and track to trick legitimate web users into providing their user credentials. Also, one website allowed the password autocomplete attribute for user credentials.

The technology security officer stated that these vulnerabilities were the result of various causes, which included programming oversight and technical issues.

These exposures increase the risk that a remote attacker may be able to exploit vulnerabilities that could lead to loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

Recommendation 9

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

In addition, we recommend that the campus ensure that departmental IT managers:

- a. Formalize a security review of critical applications and systems containing protected data for vulnerabilities prior to deployment of critical applications.
- b. Implement the campus patch management standard on all servers and network devices.
- c. Review existing web application code on a periodic basis or new code prior to deployment of critical applications or those systems containing protected data.

Campus Response

We concur.

- a. Departmental IT managers, with applications containing protected level 1 data, will develop a security review process to detect vulnerabilities by June 30, 2009.
- b. Departmental IT managers will develop an implementation plan for patch management compliance by June 30, 2009.
- c. Departmental IT managers will review existing web application code periodically and new code prior to deployment of critical applications or those systems containing protected data by June 30, 2009.

SYSTEMS SECURITY AND MONITORING

CONFIGURATION CHANGES

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

- ▶ Firewalls.
- ▶ Switches.
- ▶ Routers.
- ▶ Server/operating systems.

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

The technology security officer stated that the campus was in the process of implementing the campus IT security plan, which includes change management and process documentation.

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

Recommendation 10

We recommend that the campus:

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

Campus Response

We concur. The university will establish a process for the periodic review of network device configuration changes by June 30, 2009. The process will incorporate a formal sign-off process by appropriate personnel to ensure compliance of configuration reviews.

GRANTING OF 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.

The information security officer stated that the campus was in the process of implementing an information security plan that required compliance by all departments, including compliance with the campus standard for written management authorization for all accounts.

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

Recommendation 11

We recommend that campus establish a formal process for the management of administrative and service accounts and develop a method to track, review, and periodically audit this type of access.

Campus Response

We concur. The university will establish a process to manage administrative and service accounts by June 30, 2009.

SERVER LOG MANAGEMENT

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

The technology security officer stated that the campus was in the process of implementing an information security plan, which required formal documentation to be written for the review of server logs.

The lack of a standard process for the review of server 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 12

We recommend that the campus create a formal process to review and document the review of server logs on a periodic basis. Consideration should be given to implementation of automated log analysis and notification technologies.

Campus Response

We concur. The university will establish a process to review server logs on a periodic basis by June 30, 2009.

ROUTING AND SWITCHING DEVICES

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

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

- ▶ Two switches and the core router lacked a formal process for the granting of administrative and service accounts, which may lead to unauthorized user access to these network devices with escalated privileges.
- ▶ Four devices were configured with Simple Network Management Protocol (SNMP) version 1 or 2c, which was unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ Four devices were configured with Telecommunication Network (Telnet), which made them vulnerable to a number of packet capture attack techniques.
- ▶ Two devices did not send Transmission Control Protocol keep-alive messages for connections from a remote host, which may allow an attacker to attempt a Denial of Service by exhausting the number of possible connections.

- ▶ One device was running an outdated Internet Operating Systems version 12.1, which was susceptible to multiple vulnerabilities.

The technology security officer stated that many network devices did not support SNMP version 3 or Secure Shell version 2 and the risk was mitigated by the use of access lists, not exposing vulnerable services to the campus, and/or not using the vulnerable services. He further stated that Telnet was being eliminated on older network devices as they were being upgraded, and the other vulnerabilities were due to staff oversight.

These exposures increase the risk that a remote attacker may be able to gain access to network resources and exploit vulnerabilities that could lead to the loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

Recommendation 13

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

In addition, we recommend that the campus ensure that departmental IT managers:

- a. Formalize a security review of critical applications and systems containing protected data for vulnerabilities prior to deployment.
- b. Implement the campus patch management standard on all servers and network devices. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the live network environment to identify potential or known vulnerabilities.

Campus Response

We concur. In addition to repairing the network device vulnerabilities identified during the audit:

- a. Departmental IT managers will formalize a security review of critical applications and systems containing protected level 1 data for vulnerabilities prior to deployment by June 30, 2009.
- b. Departmental IT managers will develop an implementation plan for patch management compliance by June 30, 2009.

PROTECTED DATA

Campus reporting and investigation of protected data that might exist on lost/stolen computers was inadequate.

Our review of eight computers reported as stolen from June 2006 to April 2008 disclosed that:

- ▶ In five instances, documentation was not available to evidence the performance of proper investigation procedures and certification by the custodian that protected data was not compromised. The procedures only required verbal confirmation from the custodian of the computer as to whether unencrypted protected data was resident.
- ▶ In one instance, the reporting and investigation of the incident was not timely. Specifically, the theft occurred sometime between July 26, 2007, and August 22, 2007, and was not formally reported until September 10, 2007.
- ▶ The information security officer stated that this condition resulted because security awareness training was in the process of development to remind employees to notify the ITSO.

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

Recommendation 14

We recommend that the campus:

- a. Modify procedures to ensure that investigations of lost/stolen computers include the investigation and certification of the existence of protected data, which could include validation of the existence of confidential information through the review of backups or other verifiable methods.
- b. Ensure that incidents involving the potential loss of protected data are reported and investigated in a timely manner.

Campus Response

We concur. The university has modified its procedures to ensure that investigations of lost/stolen computers include the investigation and certification of the existence of protected data and that these incidents are reported and investigated in a timely manner.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Stephen L. Weber	President
Alan Belshaw	Information Security Professional
Scott Burns	Associate Vice President, Financial Operations
Kevin Carter	Director, Information Systems, Student Affairs
Valerie Carter	Director, Audit and Tax
Norma Casas	Analyst, Audit and Tax
Tony Chung	Director, Information Systems Management
John Denune	Technology Security Officer
Jahan Jamshidi	Director, Management Information Systems, Aztec Shops
Gene LeDuc	Security Analyst, Information Technology Security Office
Robert Newhouse	Director, University Computer Operations
Rick Nornholm	Director, Information Technology, Enrollment Services
Rich Pickett	Chief Information Officer
Mike Reeves	Director, Computing Services, San Diego State University Research Foundation
Eric Rivera	Associate Vice President, Student Affairs
John Ross	Academic Affairs Information Technology Coordinator
Sally Roush	Vice President, Business and Financial Affairs
Jim Varnell	UNIX, Windows, and Macintosh Support, College of Sciences
AJ Viado	Database Administrator, San Diego State University Research Foundation
Felecia Vlahos	Information Security Officer



San Diego State University
5500 Campanile Drive
San Diego, CA 92182-8000
Tel: 619 594-5201
Fax: 619 594-8894

THE PRESIDENT

RECEIVED
UNIVERSITY AUDITOR

March 16, 2009

MAR 17 2009

THE CALIFORNIA STATE
UNIVERSITY

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

Dear Mr. Mandel:

Attached is San Diego State University's response to Audit Report 08-18, *Information Security*. Documentation of policy and control changes will follow under separate cover.

Should you have any questions or require additional information, please contact Valerie Carter, Audit and Tax Director, at 619-594-5901.

Sincerely,

Stephen L. Weber
President

A handwritten signature in black ink, appearing to read "Steve Weber", written over a large, stylized blue scribble.

SLW:rjl

Attachment

c: Sally F. Roush, Vice President for Business and Financial Affairs
James Kitchen, Vice President for Student Affairs
Ethan Singer, Associate Vice President, Academic Affairs
Scott Burns, Associate Vice President, Financial Operations
Rich Pickett, Chief Information Officer
Valerie Carter, Director, Audit and Tax

**INFORMATION SECURITY
SAN DIEGO STATE UNIVERSITY**

Audit Report 08-18

SECURITY GOVERNANCE

SECURITY AUTHORITY AND RESPONSIBILITY

Recommendation 1

We recommend that the campus require the ITSO to routinely assess campus compliance to the information security plan.

Campus Response

We concur. The ITSO has scheduled assessments with each campus IT department. Assessments will be completed by May 29, 2009.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Recommendation 2

We recommend that the campus:

- a. Conduct a PCI assessment to determine its applicable vendor level and respective PCI requirements, and assign responsibility for ensuring that annual compliance is achieved.
- b. Complete all PCI requirements including annual risk assessments and quarterly network scans by an approved vendor, if required.

Campus Response

We concur. The University will provide a PCI assessment action plan by June 30, 2009. It will include the planned strategy, status of completion, and milestones to satisfy all PCI requirements including annual risk assessments and quarterly network scans.

RECORD RETENTION

Recommendation 3

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

Campus Response

We concur. The University will prepare a record retention action plan by July 29, 2009.

INFORMATION SECURITY AWARENESS TRAINING

Recommendation 4

We recommend that the campus develop an action plan for ensuring that all employees and contractors that have access to protected information receive information security awareness training.

Campus Response

We concur. The University will implement the CSU Security Awareness training by May 1, 2009.

EMPLOYEE SEPARATION

Recommendation 5

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

Campus Response

We concur. The University will revise the electronic manager clearance checklist to include a reminder to separating employees. The checklist will be revised by April 30, 2009.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Recommendation 6

We recommend that the campus ensure that departmental IT managers implement all aspects of the SDSU information security plan including the areas that were identified during the audit.

Campus Response

We concur. Departmental IT managers will develop an implementation plan, by June 30, 2009, for all aspects of the information security plan identified during the audit.

TECHNICAL VULNERABILITIES

Recommendation 7

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 ensure that departmental IT managers:

- a. Implement the campus patch management standard on all servers and network devices. This process would include the review of existing code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.
- b. Formalize a security review of critical applications or those systems containing protected data for security vulnerabilities prior to deployment.
- c. Implement an application development methodology to which all developers must comply prior to deploying any Internet-facing application.
- d. Comply with the security baseline standard for securing servers prior to allowing them to become Internet facing.

Campus Response

We concur. In addition to repairing all technical vulnerabilities identified:

- a. Departmental IT managers will develop an implementation plan for patch management compliance by June 30, 2009.
- b. Departmental IT managers, with applications containing protected level 1 data, will develop a security review process to detect vulnerabilities by June 30, 2009.
- c. Departmental IT managers, with Internet-facing proprietary applications, will develop a software development process by June 30, 2009.
- d. Departmental IT managers, with servers containing protected level 1 data, will develop a security review process to detect vulnerabilities by June 30, 2009.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

WEB APPLICATION DEVELOPMENT AND MAINTENANCE

Recommendation 8

We recommend that the campus ensure that departmental IT managers implement a formal software development process for critical applications or those systems containing protected data.

Campus Response

We concur. Departmental IT managers, with critical applications or containing protected level 1 data, will develop a software development process by June 30, 2009.

WEB APPLICATION VULNERABILITIES

Recommendation 9

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

In addition, we recommend that the campus ensure that departmental IT managers:

- a. Formalize a security review of critical applications and systems containing protected data for vulnerabilities prior to deployment of critical applications.
- b. Implement the campus patch management standard on all servers and network devices.
- c. Review existing web application code on a periodic basis or new code prior to deployment of critical applications or those systems containing protected data.

Campus Response

We concur.

- a. Departmental IT managers, with applications containing protected level 1 data, will develop a security review process to detect vulnerabilities by June 30, 2009.
- b. Departmental IT managers will develop an implementation plan for patch management compliance by June 30, 2009.
- c. Departmental IT managers will review existing web application code periodically and new code prior to deployment of critical applications or those systems containing protected data by June 30, 2009.

SYSTEMS SECURITY AND MONITORING

CONFIGURATION CHANGES

Recommendation 10

We recommend that the campus:

- a. Develop policies and procedures and establish a formal process for the periodic review of system configuration changes that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.

- b. Incorporate into these formal change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance of configuration reviews.

Campus Response

We concur. The University will establish a process for the periodic review of network device configuration changes by June 30, 2009. The process will incorporate a formal sign-off process by appropriate personnel to ensure compliance of configuration reviews.

GRANTING OF ADMINISTRATIVE ACCESS

Recommendation 11

We recommend that campus establish a formal process for the management of administrative and service accounts and develop a method to track, review, and periodically audit this type of access.

Campus Response

We concur. The University will establish a process to manage administrative and service accounts by June 30, 2009.

SERVER LOG MANAGEMENT

Recommendation 12

We recommend that the campus create a formal process to review and document the review of server logs on a periodic basis. Consideration should be given to implementation of automated log analysis and notification technologies.

Campus Response

We concur. The University will establish a process to review server logs on a periodic basis by June 30, 2009.

ROUTING AND SWITCHING DEVICES

Recommendation 13

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

In addition, we recommend that the campus ensure that departmental IT managers:

- a. Formalize a security review of critical applications and systems containing protected data for vulnerabilities prior to deployment.

- b. Implement the campus patch management standard on all servers and network devices. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the live network environment to identify potential or known vulnerabilities.

Campus Response

We concur. In addition to repairing the network device vulnerabilities identified during the audit:

- a. Departmental IT managers will formalize a security review of critical applications and systems containing protected level 1 data for vulnerabilities prior to deployment by June 30, 2009.
- b. Departmental IT managers will develop an implementation plan for patch management compliance by June 30, 2009.

PROTECTED DATA

Recommendation 14

We recommend that the campus:

- a. Modify procedures to ensure that investigations of lost/stolen computers include the investigation and certification of the existence of protected data, which could include validation of the existence of confidential information through the review of backups or other verifiable methods.
- b. Ensure that incidents involving the potential loss of protected data are reported and investigated in a timely manner.

Campus Response

We concur. The University has modified its procedures to ensure that investigations of lost/stolen computers include the investigation and certification of the existence of protected data and that these incidents are reported and investigated in a timely manner.



THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

May 4, 2009

CHANNEL ISLANDS

CHICO


MEMORANDUM

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed
Chancellor 

FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 08-18 on *Information Security*,
San Diego State University

LONG BEACH

LOS ANGELES

In response to your memorandum of May 4, 2009, I accept the response as submitted with the draft final report on *Information Security*, San Diego State University.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/ms

POMONA

Enclosure

SACRAMENTO

c: Mr. Scott Burns, Associate Vice President, Financial Operations
Ms. Sally F. Roush, Vice President, Business and Financial Affairs
Dr. Stephen L. Weber, President

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS