

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
NORTHRIDGE

Audit Report 08-21
February 17, 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

 Policy Issuance and Approval 8

 Payment Card Industry Data Security Standard 9

 Employee Separation..... 10

Decentralized Computing..... 10

System Development and Change Management..... 12

Systems Security and Monitoring 13

 Password Standards 13

 Granting of Administrative Access 14

 Firewalls and Routing and Switching Devices..... 14

 Network Architecture 16

 Configuration Management..... 17

 Audit and Security Event Logs Management..... 17

Protected Data 18

 System Backup Encryption 18

 Disposition of Protected Data 18

 Incident Response Management..... 19

 Lost/Stolen Computers 20

APPENDICES

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

ABBREVIATIONS

AD	Active Directory
CIO	Chief Information Officer
CSU	California State University
CSUN	California State University, Northridge
DMZ	Demilitarized Zone
HR	Human Resources
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
PCI DSS	Payment Card Industry Data Security Standard
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 California State University, Northridge campus from September 15, 2008, through October 24, 2008, and audited the procedures in effect at that time.

Our study and evaluation identified issues that, if left unattended, could 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, resource limitations often hindered or delayed information security projects and 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 October 24, 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 security officer's responsibilities depicted in the position description were not entirely consistent with those noted in the information security plan, the information security plan was not formally approved by management, and the campus did not have a formal process to evidence the ongoing review of all information security policies. Additionally, the campus and auxiliaries had not completed a Payment Card Industry Data Security Standard self-assessment questionnaire, 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 [10]

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

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [12]

Web application vulnerabilities existed on the websites selected for testing.

SYSTEM SECURITY AND MONITORING [13]

The campus password policy did not adequately address password settings, and existing password settings did not always ensure adequate security. The campus did not consistently follow existing practices for granting privileged access to firewalls and network devices. Firewalls and routing and switching devices were not always properly configured or adequately secured; and internet-accessible devices were located within the same segments as internal resources. Additionally, the campus lacked a formal process to review, approve, and retain configuration and hardening standards for network devices; and the campus lacked a formal process for the management, security, and review of network and system audit and security event logs of operating systems, servers, and applications.

PROTECTED DATA [18]

Daily backup copies for systems with protected data were not encrypted when stored locally or when in transit to California State University, Channel Islands for disaster recovery purposes. In addition, the campus could not provide evidence documenting the deletion of protected data from campus computers prior to disposal, incident response policies and procedures were inadequate and outdated, and procedures for the investigation of protected data that might exist on lost/stolen computers were 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 California State University, Northridge (CSUN), the office of IT 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 CSUN 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 security officer's responsibilities depicted in the position description were not entirely consistent with those noted in the information security plan.

Specifically, the information security officer's functions and responsibilities listed within the position description included the authority to enforce campus compliance with information security laws, rules, and regulations; however, this authority had not been communicated to the campus community within the information security plan.

The chief information officer (CIO) stated that enforcement of information security compliance is delegated to the CIO and any inconsistencies between the information security officer's position description and the responsibilities in the information security plan were inadvertently overlooked.

Inconsistencies between the information security officer's position description and the responsibilities noted in the information security plan could potentially limit the ability to direct a comprehensive system of information security management throughout the campus community. Such limitations increase campus exposure to security breaches, risk of inappropriate access to data, and could compromise compliance with statutory information security requirements.

Recommendation 1

We recommend that the campus align the responsibilities in the information security officer's position description to the responsibilities noted in the information security plan.

Campus Response

We concur. The campus has reviewed and updated the responsibilities in the information security officer's position description to align with the responsibilities noted in the information security plan.

POLICY ISSUANCE AND APPROVAL

The information security plan was not formally approved by management, and the campus did not have a formal process to evidence the ongoing review of all information security policies.

Specifically, the information security policy had not been formally reviewed since December 2002.

The CIO stated her belief that the informal processes used to approve the information security plan and to review the information security policies were sufficient.

Failure to formally approve and adequately review the information security plan and/or policies increases the risk of unauthorized exceptions, and could compromise compliance with statutory information security requirements. Such inaction may also impact the ability of the campus to opine on the overall effectiveness of existing security provisions related to such data.

Recommendation 2

We recommend that the campus issue a standard operating procedure to review and approve the information security plan, including a formal process to evidence the ongoing review of all information security policies.

Campus Response

We concur. The campus has developed and implemented a standard operating procedure to require the annual review and approval of the information security plan and information security policies. The procedure includes the requirement to document and retain evidence of the reviews for the information security plan and information security policies.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

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

The university controller stated that the lack of assessment and other actions was due to uncertainty regarding recent compliance updates to the PCI DSS requirements. He further stated that this was previously considered not to be an issue as the primary vendor that the campus used for credit card processing had been certified as complying with PCI DSS requirements.

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

Recommendation 3

We recommend that the campus complete the PCI DSS self-assessment questionnaire, define and document responsibility for assessing campus and auxiliary PCI DSS compliance, and establish a process for annual compliance review.

Campus Response

We concur. The campus will complete the PCI DSS self-assessment questionnaire, define and document responsibility for assessing campus and auxiliary PCI DSS compliance, and establish a process for annual compliance review. These will be completed by the end of June 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 manager of employee relations and workers' compensation stated that the university's confidentiality statements, (as required by Coded Memorandum HR 2005-16, *Requirements for Protecting Confidential Personal Data*) adequately inform employees of their legal responsibility to maintain the security of protected data.

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 4

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

Campus Response

We concur. The campus will modify the exit process to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data by the end of June 2009.

DECENTRALIZED COMPUTING

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

Our external testing of devices located in the decentralized network segments disclosed 52 vulnerabilities on a multitude of desktops, copiers, printers, and servers for which specific details were provided to the campus.

Additionally, the deployment of servers in the decentralized computing environment was not always adequately managed and lacked professional standards and guidance. The decentralized servers were not consistently 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 CIO stated that individual departments on campus had technical staffs that were responsible for administration of their own servers and desktops. She further stated her belief that these technical staffs were keeping their servers appropriately patched and managed.

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 5

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.
- b. Develop procedures for ensuring ongoing compliance with the campus patch management process for all machines that have access to internal network resources.
- c. Formalize a security baseline standard that requires the review of servers for security vulnerabilities prior to deployment.
- d. Develop and implement a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- e. 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 mitigate or repair all of the technical vulnerabilities identified and presented in detail by July 1, 2009.

In addition, the campus will:

- a. Develop and implement a campus-wide patch management process that includes the review of existing web application code and network-device configuration code on a periodic basis or new code prior to deployment into the production environment by July 1, 2009.
- b. Develop procedures to ensure ongoing compliance with the campus-wide patch management process for all machines that have access to internal network resources by July 1, 2009.

- c. Develop a procedure and security baseline standard that requires the review of servers for security vulnerabilities prior to deployment and prior to becoming Internet facing by July 1, 2009.
- d. Develop and implement a campus-wide application development standard to which all developers must comply with prior to deploying an Internet-facing application by the end of July 1, 2009.
- e. Provide the ancillary IT units with the procedure and security baseline standard that requires the review of servers for security vulnerabilities prior to deployment and prior to becoming Internet facing by July 1, 2009.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

Web application vulnerabilities existed on the website selected for testing.

Our review of the selected website disclosed three vulnerabilities for which specific details were provided to the campus.

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

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 6

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

In addition, we recommend that the campus:

- a. Formalize a security standard that requires the review of applications for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.
- c. Develop procedures for ensuring ongoing compliance with the campus patch management process for all machines that have access to internal network resources.

Campus Response

We concur. The campus will repair or mitigate the website vulnerabilities identified and presented in detail by July 1, 2009.

In addition, the campus will:

- a. Develop a security standard that requires the review of applications for security vulnerabilities prior to deployment by July 1, 2009.
- b. Develop and implement a campus-wide patch management process that includes the review of existing web application code on a periodic basis or new code prior to deployment into the production environment by July 1, 2009.
- c. Develop procedures to ensure ongoing compliance with the campus patch management process for all machines that have access to internal network resources by July 1, 2009.

SYSTEMS SECURITY AND MONITORING

PASSWORD STANDARDS

The campus password policy did not adequately address password settings, and existing password settings did not always ensure adequate security.

Specifically, existing password settings in the password policy did not always ensure adequate security was enforced within the Lightweight Directory Access Protocol or Active Directory (AD) group policy for password management.

The interim information security officer stated his belief that the current campus password policy was sufficient.

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

Recommendation 7

We recommend that the campus:

- a. Implement a formal password policy to govern all campus systems and incorporate it into the existing IT security policy.

- b. Review the current enterprise AD and departmental server policy settings and develop a threshold that adequately balances security and business enablement across the enterprise environment.

Campus Response

We concur. The campus will:

- a. Implement a formal password policy to govern all campus systems and incorporate it into the existing IT security policy by July 1, 2009.
- b. Review the current enterprise AD and departmental policy settings and develop a threshold that adequately balances security and business enablement across the enterprise environment by July 1, 2009.

GRANTING OF ADMINISTRATIVE ACCESS

The campus did not consistently follow existing practices for granting privileged access to firewalls and network devices.

The senior director of infrastructure services stated that this finding resulted from not having a formal process in place for granting privileged access to network devices.

The lack of adherence to the formal process for granting privileged access may lead to inadequate segregation of duties, the granting of accounts not based on the principle of least privilege, and/or unauthorized access.

Recommendation 8

We recommend that the campus ensure that the formal process for the granting of privileged accounts be adhered to for all systems and equipment.

Campus Response

We concur. The campus will update and formalize its procedures for granting privileged accounts to include all systems and equipment by July 1, 2009.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

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

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

- ▶ Three devices were enabled with Telecommunication Network (Telnet), which could allow a remote attacker to obtain confidential authentication tokens to permit remote access to the devices in question as user logins, passwords, and commands are transferred across the network in clear text.
- ▶ Two devices were configured to use clear-text Simple Network Management Protocol (SNMP) versions 1 and 2c, which were unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ One device was enabled with unencrypted password storage on its configuration file, which could allow an attacker with access to the device's configuration to quickly extract clear text passwords without having to decode or brute-force them.
- ▶ One device supported a vulnerable version of Secure Shell Protocol, which could allow an attacker to gain execution capabilities on the device.
- ▶ One device was configured with no access control list to restrict administrative access, which could permit an attacker full administrative access to the device.

The senior director of infrastructure services stated that mitigating controls were in place to minimize the risk of using SNMP v2 and Telnet and that the remaining findings resulted from not having a formal configuration review process in place.

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 9

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:

- a. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. 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.
- c. Develop procedures for ensuring ongoing compliance with the campus patch management process for all machines that have access to internal network resources.

Campus Response

We concur. The campus will repair or mitigate the network device vulnerabilities identified and presented in detail by July 1, 2009.

In addition, the campus will:

- a. Develop a security standard that requires the review of network devices for security vulnerabilities prior to deployment by June 2009.
- b. Develop and implement a campus-wide patch management process that includes the review of existing network-device configuration code on a periodic basis or new configuration code prior to deployment into the production environment to identify potential or known vulnerabilities by July 1, 2009.
- c. Develop procedures to ensure ongoing compliance with the campus patch management process for all machines that have access to internal network resources by July 1, 2009.

NETWORK ARCHITECTURE

Internet-accessible devices were located within the same segments as internal resources.

Normally, these Internet-accessible devices are segmented into a demilitarized zone (DMZ) such that if these devices were compromised, there would be separation among other internal network resources.

The senior director of infrastructure services stated that the Internet-accessible devices were not always segmented from internal network resources because a complete inventory of all Internet-accessible devices had not been completed to identify those that needed to be in the DMZ or otherwise segmented.

Inadequate segmentation of publicly accessible devices from internal resources increases the risk that compromised devices could be used to pivot to other network targets and launch attacks against internal resources if a layered security model is not used.

Recommendation 10

We recommend that the campus review its current network topology and determine how to best logically separate Internet-accessible devices from devices residing within the internal network.

Campus Response

We concur. The campus will review its network topology to determine how to best logically configure the Internet-accessible devices from devices residing within the internal network by July 1, 2009.

CONFIGURATION MANAGEMENT

The campus lacked a formal process to review, approve, and retain configuration and hardening standards for network devices.

The CIO stated that the campus had not considered it a necessity to formally document all of its processes.

Inadequate configuration management increases the risk that network devices are not securely configured.

Recommendation 11

We recommend that the campus create a formal process to review, approve, and retain the configuration and hardening standards for network devices that are outlined in the IT security plan.

Campus Response

We concur. The campus will create a formal process to review, approve, and retain the configuration and hardening standards for network devices by June 1, 2009.

AUDIT AND SECURITY EVENT LOGS MANAGEMENT

The campus lacked a formal process for the management, security, and review of network and system audit and security event logs of operating systems, servers, and applications.

Individual custodians of operating systems, servers, and applications were responsible for determining and implementing estimated best practices for log management with no general oversight or direction from IT.

The senior director of infrastructure services stated his belief that the current process for managing, securing, and reviewing system and network logs was sufficient.

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

Recommendation 12

We recommend that the campus develop guidelines for the management, security, and review of audit logs and security event logs of operating systems, servers, and applications 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.

Campus Response

We concur. The campus will develop guidelines for the management, security, and review of audit logs and security event logs of operating systems, servers, and applications to assist in identifying potential network vulnerabilities and breaches on campus systems. This process will consider the use of tools and analytical methods, personnel responsibilities, frequency, and reporting/escalating processes. The guidelines will be developed by July 1, 2009.

PROTECTED DATA

SYSTEM BACKUP ENCRYPTION

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

The senior director of infrastructure services stated that the campus' current backup solution did not accommodate encryption.

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

Recommendation 13

We recommend that the campus encrypt system backups with protected data when stored locally and at all off-site storage locations.

Campus Response

We concur. The campus will implement a backup encryption solution and will encrypt system backups that contain protected data when stored locally and at all off-site storage locations by July 1, 2009.

DISPOSITION OF PROTECTED DATA

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

We reviewed eight computers that were disposed of from 2005 to 2008 and found that the campus was unable to provide any evidence of hard-drive wiping.

The CIO stated that the hard-drive wiping of campus computers with protected data prior to disposal was generally practiced; however, it was not formally documented in all cases.

Inadequate control over equipment assets, especially those containing protected data, increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

Recommendation 14

We recommend that the campus amend their practices for the disposal/transfer of computers that contain confidential information to ensure that hard-drive wiping is sufficiently documented, including retention of the documentation.

Campus Response

We concur. The campus will document its procedure for the disposal/transfer of computers that contain confidential information. The procedure will include the requirement to document and retain evidence of hard-drive wiping. The procedure will be developed by June 1, 2009.

INCIDENT RESPONSE MANAGEMENT

The campus incident response policies and procedures were inadequate and outdated.

We found that:

- ▶ Low-risk security incidents dated between September 1, 2006, and September 9, 2008, were not closed until 1 to 309 days subsequent to their creation dates. In addition, there were no documented procedures defining the time frame within which low-risk security incidents should be investigated and reviewed by management, and no evidence of managerial review.
- ▶ There was no evidence that third-party users and contractors were informed of their incident response responsibilities and the process for reporting security events.
- ▶ Neither the information security incidence response standard operating procedure nor the information security policies addressed when and how to engage legal counsel during a security incident.
- ▶ Campus policies and procedures related to information security incident response had not been formally reviewed since their effective dates, which ranged from 2004 to 2006.

The CIO stated her belief that the existing documents and practices were adequate and that as CIO she could contact legal counsel as needed.

Inadequate and outdated incident response policies and procedures increase the risk that information security breaches could go unreported, which could compromise compliance with statutory information security requirements and damage the campus' reputation.

Recommendation 15

We recommend that the campus:

- a. Ensure that low-risk security incidents are timely investigated and reviewed, including evidence of managerial review.
- b. Review policies and procedures related to information security incident response and update as necessary, including evidence that third-party users and contractors are informed of their incident response responsibilities and the process for reporting security events and protocol related to when and how to engage legal counsel during a security incident.

Campus Response

We concur.

- a. The campus will update its incident response procedure to include language about the timely investigation and managerial review of security incidents by May 1, 2009.
- b. The campus has developed and implemented a procedure to annually review its information security policies and procedures and update as necessary.
- c. The campus has updated its incident response procedure to include language about engaging legal counsel as necessary during a security incident.
- d. The campus has updated its vendor/contractor purchase order language so that vendors/contractors are informed of their incident response responsibilities and the process for reporting security events.
- e. The campus will update its guest/third-party account-issuance procedure to include language that informs guests/third-party users of their incident response responsibilities and the process for reporting security events by June 1, 2009.

LOST/STOLEN COMPUTERS

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

Our review of ten computers reported as lost or stolen from April 2006 to March 2008 disclosed that:

- ▶ In nine instances, there was no evidence on file to show that the first responders to computer theft investigations inquired about the potential compromise of protected data or the campus efforts to notify affected parties of potential losses.

- ▶ In one instance, the reported incident was not reported and formally investigated until nine days after the incident occurred.

The chief of police stated that California State University, Northridge police officers generally asked for this information; however, it was not formally documented in all cases.

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.

Recommendation 16

We recommend that the campus develop and implement a computer loss/theft procedure to ensure that the investigation and certification of the existence of protected data is sufficiently documented and retained, and coordinated with the information security office.

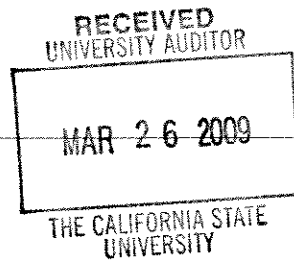
Campus Response

We concur. The campus has developed and implemented a computer loss/theft procedural directive to ensure that the investigation and certification of the existence of protected data on stolen computing hardware is sufficiently documented, retained, and coordinated with the information security office.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Jolene Koester	President
Hilary Baker	Vice President, Information Technology and Chief Information Officer
Robert Barker	University Controller
Sylvia Barnes	Information Security Specialist
Anne Glavin	Chief of Police
Hien Ho	Senior Director, Infrastructure Services
Kevin Krzewinski	Director, Application Development Services
Danita Leese	Executive Analyst
Howard Lutwak	Director, Internal Audit
Tom McCarron	Interim Vice President, Administration and Finance and Chief Financial Officer
Will Moran	Network Engineering Lead
Gregory Nicols	Director, Telecomm and Systems Administration
Christian Olsen	Interim Information Security Officer
Benjamin Quillian	Senior Director, Administration and User Support Services (At time of review)
Jill Smith	Manager, Employee Relations and Workers' Compensation
Chris Xanthos	Director, Project Management Office

California State University
Northridge



Office of the Vice President
 Administration and Finance

March 26, 2009

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

Subject: Campus Response to Recommendations of Audit Report Number 08-21
Information Security at California State University, Northridge

Dear Larry:

Enclosed please find the California State University, Northridge (CSUN) response to the recommendations of the audit, as requested in your letter of February 26, 2009. We have also sent this document via e-mail to adouglas@calstate.edu.

We have read the report including the observations and recommendations, and agree with them. Corrective action to implement all of the recommendations is being implemented. By separate correspondence, the applicable documents evidencing completion of our implementation process and corrective action for each recommendation will be provided.

Should there be questions regarding the contents of the response, they may be addressed to Howard Lutwak, Director of Internal Audit at (818) 677-7647.

We appreciate the recommendations to improve CSUN's systems of internal control.

Sincerely,

Tom McCarron
 Vice President Administration and Finance
 and CFO

Enclosures

cc: Dr. Jolene Koester, President
 Howard Lutwak, Director of Internal Audit

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
NORTHRIDGE

Audit Report 08-21

SECURITY GOVERNANCE

SECURITY AUTHORITY AND RESPONSIBILITY

Recommendation 1

We recommend that the campus align the responsibilities in the information security officer's position description to the responsibilities noted in the information security plan.

Campus Response

We concur.

The campus has reviewed and updated the responsibilities in the information security officer's position description to align with the responsibilities noted in the information security plan.

POLICY ISSUANCE AND APPROVAL

Recommendation 2

We recommend that the campus issue a standard operating procedure to review and approve the information security plan, including a formal process to evidence the ongoing review of all information security policies.

Campus Response

We concur.

The campus has developed and implemented a standard operating produce to require the annual review and approval of the information security plan and information security policies. The procedure includes the requirement to document and retain evidence of the reviews for the information security plan and information security policies.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Recommendation 3

We recommend that the campus complete the PCI DSS self-assessment questionnaire, define and document responsibility for assessing campus and auxiliary PCI DSS compliance, and establish a process for annual compliance review.

Campus Response

We concur. The campus will complete the PCI DSS self-assessment questionnaire, define and document responsibility for assessing campus and auxiliary PCI DSS compliance, and establish a process for annual compliance review. These will be completed by the end of June 2009.

EMPLOYEE SEPARATION

Recommendation 4

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

Campus Response

We concur. The campus will modify the exit process to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data by the end of June 2009.

DECENTRALIZED COMPUTING

Recommendation 5

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.
- b. Develop procedures for ensuring ongoing compliance with the campus patch management process for all machines that have access to internal network resources.
- c. Formalize a security baseline standard that requires the review of servers for security vulnerabilities prior to deployment.
- d. Develop and implement a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- e. 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 mitigate or repair all of the technical vulnerabilities identified and presented in detail by July 1, 2009.

In addition, the campus will:

- a. Develop and implement a campus-wide patch management process that includes the review of existing web application code and network-device configuration code on a periodic basis or new code prior to deployment into the production environment by July 1, 2009.
- b. Develop procedures to ensure ongoing compliance with the campus-wide patch management process for all machines that have access to internal network resources by July 1, 2009.
- c. Develop a procedure and security baseline standard that requires the review of servers for security vulnerabilities prior to deployment and prior to becoming Internet facing by July 1, 2009.
- d. Develop and implement a campus-wide application development standard to which all developers must comply with prior to deploying an Internet-facing application by the end of July 1, 2009.
- e. Provide the ancillary IT units with the procedure and security baseline standard that requires the review of servers for security vulnerabilities prior to deployment and prior to becoming Internet facing by July 1, 2009

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

Recommendation 6

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

In addition, we recommend that the campus:

- a. Formalize a security standard that requires the review of applications for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.
- c. Develop procedures for ensuring ongoing compliance with the campus patch management process for all machines that have access to internal network resources.

Campus Response

We concur. The campus will repair or mitigate the website vulnerabilities identified and presented in detail by July 1, 2009.

In addition, the campus will:

- a. Develop a security standard that requires the review of applications for security vulnerabilities prior to deployment by July 1, 2009.

- b. Develop and implement a campus-wide patch management process that includes the review of existing web application code on a periodic basis or new code prior to deployment into the production environment by July 1, 2009.
- c. Develop procedures to ensure ongoing compliance with the campus patch management process for all machines that have access to internal network resources by July 1, 2009.

SYSTEMS SECURITY AND MONITORING

PASSWORD STANDARDS

Recommendation 7

We recommend that the campus:

- a. Implement a formal password policy to govern all campus systems and incorporate it into existing IT security policy.
- b. Review the current enterprise AD and departmental server policy settings and develop a threshold that adequately balances security and business enablement across the enterprise environment.

Campus Response

We concur.

The campus will:

- a. Implement a formal password policy to govern all campus systems and incorporate it into the existing IT security policy by July 1, 2009.
- b. Review the current enterprise AD and departmental policy settings and develop a threshold that adequately balances security and business enablement across the enterprise environment by July 1, 2009.

GRANTING OF ADMINISTRATIVE ACCESS

Recommendation 8

We recommend that campus ensure that the formal process for the granting of privileged accounts be adhered to for all systems and equipment.

Campus Response

We concur.

The campus will update and formalize its procedures for granting privileged accounts to include all systems and equipment by July 1, 2009.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

Recommendation 9

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:

- a. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. 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.
- c. Develop procedures for ensuring ongoing compliance with the campus patch management process for all machines that have access to internal network resources.

Campus Response

We concur. The campus will repair or mitigate the network device vulnerabilities identified and presented in detail by July 1, 2009.

In addition, the campus will:

- a. Develop a security standard that requires the review of network devices for security vulnerabilities prior to deployment by June 2009.
- b. Develop and implement a campus-wide patch management process that includes the review of existing network-device configuration code on a periodic basis or new configuration code prior to deployment into the production environment to identify potential or known vulnerabilities by July 1, 2009.
- c. Develop procedures to ensure ongoing compliance with the campus patch management process for all machines that have access to internal network resources by July 1, 2009.

NETWORK ARCHITECTURE

Recommendation 10

We recommend that the campus review its current network topology and determine how to best logically separate Internet accessible devices from devices residing within the internal network.

Campus Response

We concur. The campus will review its network topology to determine how to best logically configure the Internet accessible devices from devices residing within the internal network by July 1, 2009.

CONFIGURATION MANAGEMENT

Recommendation 11

We recommend that the campus create a formal process to review, approve, and retain the configuration and hardening standards for network devices that are outlined in the IT security plan.

Campus Response

We concur. The campus will create a formal process to review, approve, and retain the configuration and hardening standards for network devices by June 1, 2009.

AUDIT AND SECURITY EVENT LOGS MANAGEMENT

Recommendation 12

We recommend that the campus develop guidelines for the management, security, and review of audit logs and security event logs of operating systems, servers, and applications 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.

Campus Response

We concur.

The campus will develop guidelines for the management, security, and review of audit logs and security event logs of operating systems, servers, and applications to assist in identifying potential network vulnerabilities and breaches on campus systems. This process will consider the use of tools and analytical methods, personnel responsibilities, frequency, and reporting/escalating processes. The guidelines will be developed by July 1, 2009.

PROTECTED DATA

SYSTEM BACKUP ENCRYPTION

Recommendation 13

We recommend that the campus encrypt system backups with protected data when stored locally and at all off-site storage locations.

Campus Response

We concur. The campus will implement a backup encryption solution and will encrypt system backups that contain protected data when stored locally and at all off-site storage locations by July 1, 2009.

DISPOSITION OF PROTECTED DATA

Recommendation 14

We recommend that the campus amend their practices for the disposal/transfer of computers that contain confidential information to ensure that hard drive wiping is sufficiently documented, including retention of the documentation.

Campus Response

We concur. The campus will document its procedure for the disposal/transfer of computers that contain confidential information. The procedure will include the requirement to document and retain evidence of hard drive wiping. The procedure will be developed by June 1, 2009.

INCIDENT RESPONSE MANAGEMENT

Recommendation 15

We recommend that the campus:

- a. Ensure that low risk security incidents are timely investigated and reviewed, including evidence of managerial review.
- b. Review policies and procedures related to information security incident response and update as necessary, including evidence that third-party users and contractors are informed of their incident response responsibilities and the process for reporting security events and protocol related to when and how to engage legal counsel during a security incident.

Campus Response

We concur.

- a. The campus will update its incident response procedure to include language about the timely investigation and managerial review of security incidents by May 1, 2009.
- b. The campus has developed and implemented a procedure to annually review its Information Security policies and procedures and update as necessary.
- c. The campus has updated its incident response procedure to include language about engaging legal counsel as necessary during a security incident.
- d. The campus has updated its vendor/contractor Purchase Order language so that vendors/contractors are informed of their incident response responsibilities and the process for reporting security events.
- e. The campus will update its guest/ third party account-issuance procedure to include language that informs guests/ third party users of their incident response responsibilities and the process for reporting security events by June 1, 2009.

LOST/STOLEN COMPUTERS

Recommendation 16

We recommend that the campus develop and implement a computer loss/theft procedure to ensure that the investigation and certification of the existence of protected data is sufficiently documented and retained, and coordinated with the information security office.

Campus Response

We concur.

The campus has developed and implemented a computer loss/theft procedural directive to ensure that the investigation and certification of the existence of protected data on stolen computing hardware is sufficiently documented, retained, and coordinated with the information security office.



THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

May 4, 2009

CHANNEL ISLANDS

CHICO

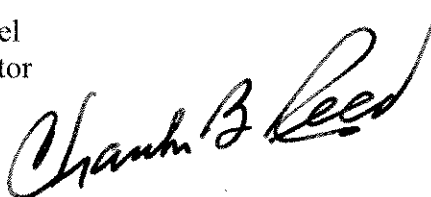
MEMORANDUM

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed
Chancellor


FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 08-21 on *Information Security*,
California State University, Northridge

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*, California State University, Northridge.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/ms

POMONA

Enclosure

SACRAMENTO

c: Dr. Jolene Koester, President
Mr. Howard Lutwak, Director, Internal Audit

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS