SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA STATE UNIVERSITY,
FULLERTON

Audit Report 11-51
November 18, 2011

Members, Committee on Audit

Henry Mendoza, Chair
Melinda Guzman, Vice Chair
Margaret Fortune  Steven M. Glazer
William Hauck   Hsing Kung   Linda Lang

Staff

University Auditor:  Larry Mandel
Senior Director:  Michael Caldera
IT Audit Manager:  Greg Dove
Senior Auditor:  Gordon Eng

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
APPENDICES

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

ABBREVIATIONS

CSU California State University
ICSUAM Integrated California State University Administrative Manual
IT Information Technology
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2010, the Board of Trustees, at its January 2011 meeting, directed that Sensitive Data Security and Protection be reviewed. The Office of the University Auditor had previously reviewed some aspects of sensitive data in the 2008 and 2009 audits of Information Security.

We visited the California State University, Fullerton campus from July 5, 2011, through July 29, 2011, and audited the procedures in effect at that time.

Our study and evaluation did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on controls over sensitive data. However, we did identify other reportable weaknesses that are described in the executive summary and body of this report. In our opinion, the operational and administrative controls over sensitive data in effect as of July 29, 2011, taken as a whole, were sufficient to meet the objectives stated in the “Purpose” section of this report.

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 controls over sensitive data, but was designed to assess management controls, increase awareness of the topic, and assess regulatory compliance for significant sensitive data categories that are prevalent in the California State University (CSU) 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.

DATA CLASSIFICATION [6]

Administration of paper documents containing sensitive information needed improvement. Specifically, the campus information security program did not include the identification of paper documents containing sensitive data, and the security of that data had not been validated by the information security office.

HUMAN RESOURCE SECURITY [7]

Background checks were not being performed for campus student assistants who had access to level one data as defined in the California State University Data Classification Standard.
APPLICATION SYSTEM ACCESS [7]

Access to social security numbers were not appropriately restricted to only authorized personnel, and the annual system access evaluation process did not include a review of access to social security numbers.
INTRODUCTION

BACKGROUND

Integrated California State University Administrative Manual (ICSUAM) §8000.0, Information Security Policy, dated April 19, 2010, represents the most recent and specific guidance to campuses regarding security and protection of sensitive data. It provides direction for managing and protecting the confidentiality, integrity and availability of California State University (CSU) information assets and defines the organizational scope of information security throughout the system.

The policy states that the Board of Trustees is responsible for protecting the confidentiality, integrity and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

According to ICSUAM §8000.0, it is the collective responsibility of all users to ensure:

- The confidentiality of information that the CSU must protect from unauthorized access.

- The integrity and availability of information stored on or processed by CSU information systems.

- Compliance with applicable laws, regulations, and CSU or campus policies governing information security and privacy protection.

It further states that auxiliary organizations, external businesses and organizations that use campus information assets must also follow the CSU Information Security Policy.

State Administrative Manual §5300 defines information security as the protection of information and information systems and equipment 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 §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 in the California Office of Information Security.

At the CSU campuses, the information security officer has overall responsibility for the security and protection of sensitive data, which extends to all campus departments, colleges and auxiliary organizations.
Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration and control of sensitive data; to determine the adequacy of controls over the related processes; 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 responsible for achieving and maintaining appropriate protection of organizational assets, and information is appropriately classified to indicate the expected degree of protection.

- Security responsibilities are addressed with employees prior to the start of employment so that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work.

- 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 systems, applications, and business processes surrounding sensitive data are controlled by means of user identification and authentication, based on business and security requirements.

- Formal event reporting and escalation procedures are in place for information security events and weaknesses, and communication is consistent and effective, allowing for timely corrective action.

- The information systems’ design, configuration, operation, use, and management are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.

- Contractual language addressing a third party’s responsibility for protecting sensitive data is appropriate.
SCOPE AND METHODOLOGY

The proposed scope of the audit, as presented in Action Item, Agenda Item 2 of the January 25 and 26, 2011, meeting of the Committee on Audit, stated that sensitive data security and protection would include review and compliance with Trustee policy, federal and state directives, and campus policies and procedures; procedures for handling confidential information; communication and employee training; encryption; tracking and monitoring of access to sensitive data; and retention practices for key records. If the sensitive data is maintained by a third party, we would review the involvement of campus information security personnel in the decision process; documentation of campus expectations for handling and securing the data; contract language covering security expectations; and monitoring of third-party performance.

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 administrative, compliance, and operational, and technical controls over the security and protection of sensitive data. 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.
- Access and configuration controls over networks, systems, applications, business processes, and data.
- Incident response, escalation, and reporting procedures.
- Compliance with relevant statutory, regulatory, and contractual security requirements.
- Third-party contractual language regarding handling of sensitive data.

Our testing and methodology was designed to provide a managerial level review of key security practices over sensitive data. Our review did not examine all categories of sensitive data; selected emerging technologies were excluded from the scope of the review. Our testing approach was designed to provide a view of the security used to protect only key computing and business processes.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

DATA CLASSIFICATION

Administration of paper documents containing sensitive information needed improvement.

We found that the campus information security program did not include the identification of paper documents containing sensitive data, and the security of that data had not been validated by the information security office.

Integrated California State University Administrative Manual (ICSUAM) §8010, Minimum Requirements for Information Security Programs, dated April 19, 2010, states, in part, that each campus president and the assistant vice chancellor for information technology services are responsible for the establishment and implementation of an information security program that contains administrative, technical, and physical safeguards designed to protect campus information assets. Each campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The program should, among other things: a) provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic), and b) develop risk management strategies to identify and mitigate threats and vulnerabilities.

The vice president of information technology (IT) stated that the information security program was being implemented in various stages, and the scoping of hard paper documentation had not been included yet.

Failure to identify and assess the risk of paper documents within the full scope of the information security program could lead to inappropriate exposure of sensitive data.

Recommendation 1

We recommend that the campus expand the information security program to include the identification of paper documents containing sensitive data and ensure that they are appropriately secured.

Campus Response

We concur. The campus, by April 1, 2012, will expand the information security program to include the identification of paper documents containing sensitive data and ensure that they are appropriately secured.
HUMAN RESOURCE SECURITY

Background checks were not being performed for campus student assistants who had access to level one sensitive data as defined in the California State University (CSU) Data Classification Standard.

ICSUAM §8030, Personnel Information Security, dated April 19, 2010, states that campuses must develop procedures to conduct background checks on positions involving access to level one information assets as defined in the CSU Data Classification Standard.

The executive assistant to the president stated that the failure to perform background checks on students with access to level one sensitive data was due to oversight.

Failure to perform background checks on personnel who have access to sensitive data increases the risk of potential mishandling and inappropriate disclosure of sensitive data.

Recommendation 2

We recommend that the campus perform background checks on campus student assistants who have access to level one sensitive data.

Campus Response

We concur. The campus, by April 1, 2012, will integrate background checks on campus student assistants who require access to level one sensitive data into the existing student assistant hiring process.

APPLICATION SYSTEM ACCESS

Access to social security numbers was not appropriately restricted to only authorized personnel, and the annual system access evaluation process did not include a review of access to social security numbers.

We found that employees from several campus departments, such as geography, history, and biology, had access that allowed them to view social security numbers.

ICSUAM §8060, Access Control, dated April 19, 2010, states that access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task.

State Administrative Manual §4841 states that state agencies must provide for the proper use and protection of information assets by establishing appropriate policies and procedures for preserving the integrity and security of automated files and databases.
The vice president of IT stated that some unauthorized personnel may have had access to certain sensitive data because preset roles assign to some employees access that they do not need.

Improper assignment of employee access could lead to unauthorized or inappropriate disclosure of sensitive data and could adversely affect campus compliance with statutory regulations regarding protection of such data.

**Recommendation 3**

We recommend that the campus:

a. Appropriately restrict access to social security numbers to only authorized personnel.

b. Expand the annual system access evaluation process to include a review of access to social security numbers.

**Campus Response**

We concur.

a. The campus, by April 1, 2012, will update the current ERP access request process and will require justification by the individual’s appropriate administrator for access, indirect and direct, to any ERP roles giving access to full social security numbers.

b. The campus information security office, by April 1, 2012, will integrate the verification of employee access to full social security numbers into the annual ERP access control review process.
## APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Milton A. Gordon</td>
<td>President</td>
</tr>
<tr>
<td>Silas Abrego</td>
<td>Vice President for Student Affairs</td>
</tr>
<tr>
<td>Ryan Alcantara</td>
<td>Associate Vice President for Student Affairs</td>
</tr>
<tr>
<td>Amy Alspaugh</td>
<td>Assistant to the Associate Vice President of Academic Affairs</td>
</tr>
<tr>
<td>Welson Badal</td>
<td>Director, Administration and Finance Information Technology (IT)</td>
</tr>
<tr>
<td>William Barrett</td>
<td>Associate Vice President for Administration and Finance</td>
</tr>
<tr>
<td>John Beisner</td>
<td>Director, University Risk Management</td>
</tr>
<tr>
<td>Kerry Boyer</td>
<td>Director, IT Information Security</td>
</tr>
<tr>
<td>Pat Carroll</td>
<td>Executive Assistant to the President</td>
</tr>
<tr>
<td>Amir Dabirian</td>
<td>Vice President, IT</td>
</tr>
<tr>
<td>Nancy Dority</td>
<td>Assistant Vice President of Enrollment Services</td>
</tr>
<tr>
<td>Naomi Goodwin</td>
<td>Assistant Vice President for Administration and Finance</td>
</tr>
<tr>
<td>Willie Hagan</td>
<td>Vice President, Administration and Finance/Chief Financial Officer</td>
</tr>
<tr>
<td>Bahram Hatefi</td>
<td>Director of Internal Audit</td>
</tr>
<tr>
<td>Rommel Hildago</td>
<td>Assistant Vice Director for IT and Senior Director for Infrastructure</td>
</tr>
<tr>
<td>Elizabeth Housewright</td>
<td>Associate University Librarian</td>
</tr>
<tr>
<td>Terry Jarmon</td>
<td>IT Asset Security and Reprographics Manager</td>
</tr>
<tr>
<td>Denise Johnson</td>
<td>Director, Human Resource Operations</td>
</tr>
<tr>
<td>Chris Manriquez</td>
<td>Associate Vice President, IT</td>
</tr>
<tr>
<td>Tariq Marji</td>
<td>Chief Financial Officer, CSU, Fullerton, Auxiliary Services Corporation</td>
</tr>
<tr>
<td>Mary Jo Medyn</td>
<td>Assistant to Vice President of Academic Affairs</td>
</tr>
<tr>
<td>Ron Morris</td>
<td>IT Systems Administrator, Associated Students California State University, Fullerton, Inc.</td>
</tr>
<tr>
<td>Frank Mumford</td>
<td>Executive Director, CSU, Fullerton, Auxiliary Services Corporation</td>
</tr>
<tr>
<td>Steve Murray</td>
<td>Acting Vice President of Academic Affairs</td>
</tr>
<tr>
<td>Willie Peng</td>
<td>Assistant Director, Infrastructure Services</td>
</tr>
<tr>
<td>Blanca Rodriguez</td>
<td>Payroll Director</td>
</tr>
<tr>
<td>Fred Sanchez</td>
<td>Executive Director, Associated Students California State University, Fullerton, Inc.</td>
</tr>
<tr>
<td>Ira Unterman</td>
<td>Chief Financial Officer, CSU Fullerton Philanthropic Foundation and Executive Director for Advancement Operations, California State University, Fullerton</td>
</tr>
</tbody>
</table>
DATE: November 29, 2011

TO: Larry Mandel, University Auditor

FROM: Milton Gordon, CSUF President

SUBJECT: Campus Response for the Sensitive Data Security and Protection Audit Report 11-51

I am pleased to forward California State University, Fullerton's official response to the three (3) recommendations in the Sensitive Data Security and Protection Audit Report 11-51.

Once again, we would like to thank the University Auditor and his staff for conducting the audit in a professional manner in identifying meaningful ways to improve the operational and administrative controls for Sensitive Data Security and Protection to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor Directives, and campus procedures.

The Campus Auditor, Bahram Hatefi, will also forward the responses to you electronically for your convenience. Should you have questions, please contact Bahram at (657) 278-7299 or bhatefi@fullerton.edu.

Attachments

cc: Pat Carroll, Executive Assistant to the President
    Amir Dabirian, Vice President for Information Technology and CITO
    Bahram Hatefi, Director of CSUF Internal Audit
    Kerry Boyer, Director, IT Information Security
SENSITIVE DATA SECURITY AND PROTECTION

CALIFORNIA STATE UNIVERSITY, FULLERTON

Audit Report 11-51

DATA CLASSIFICATION

Recommendation 1

We recommend that the campus expand the information security program to include the identification of paper documents containing sensitive data and ensure that they are appropriately secured.

Campus Response

We concur. The campus, by April 1, 2012, will expand the information security program to include the identification of paper documents containing sensitive data and ensure that they are appropriately secured.

HUMAN RESOURCE SECURITY

Recommendation 2

We recommend that the campus perform background checks on campus student assistants who have access to level one sensitive data.

Campus Response

We concur. The campus, by April 1, 2012, will integrate background checks on campus student assistants who require access to level one sensitive data into the existing student assistance hiring process.

APPLICATION SYSTEM ACCESS

Recommendation 3

We recommend that the campus:

a. Appropriately restrict access to social security numbers to only authorized personnel.

b. Expand the annual system access evaluation process to include a review of access to social security numbers.
Campus Response

a. We concur. The campus, by April 1, 2012, will update the current ERP access request process and will require justification by the individual’s appropriate administrator for access, indirect and direct, to any ERP roles giving access to full social security numbers.

b. We concur. The campus Information Security Office, by April 1, 2012, will integrate the verification of employee access to full social security numbers into the annual ERP access control review process.
January 3, 2012

MEMORANDUM

TO: Mr. Larry Mandel
    University Auditor

FROM: Charles B. Reed
      Chancellor

SUBJECT: Draft Final Report 11-51 on
          Sensitive Data Security and Protection,
          California State University, Fullerton

In response to your memorandum of January 3, 2012, I accept the response as submitted with the draft final report on Sensitive Data Security and Protection, California State University, Fullerton.

CBR/amd