SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

June 28, 2013

WILLIAM S. HODGKISS
Associate Vice Chancellor
Academic Affairs
0001

Subject: ***Academic Affairs Distributed Network Security – Phase II***
Audit Project 2013-32

The final audit report for *Academic Affairs Distributed Network Security – Phase II,* Audit Report 2013-32, is attached. We would like to thank all members of the divisions included in the scope of the review for their cooperation and assistance.

The findings included in this report will be added to our follow-up system. We will schedule a review of the management corrective actions at the appropriate time.

UC wide policy requires that all draft audit reports, both printed (copied on tan paper for ease of identification) and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS or destroy them at this time.

David Meier
Assistant Vice Chancellor
Audit & Management Advisory Services

Attachment

cc: D. Larson
G. Matthews
D. McGraw
S. Subramani
S. Vacca

UC San Diego

AUDIT & MANAGEMENT ADVISORY SERVICES

Academic Affairs Distributed Network Security – Phase II
May 2013

Performed By:

Greg Buchanan, Auditor
Daren Kinser, Auditor

Approved By:

David Meier, Assistant Vice Chancellor

Project Number: 2013-32

Academic Affairs Distributed Network Security – Phase II
Audit & Management Advisory Services Project 2013-32

Table of Contents

Academic Affairs Distributed Network Security – Phase II
Audit & Management Advisory Services Project 2013-32

I. Background

Audit & Management Advisory Services (AMAS) completed Phase II of the Academic Affairs Distributed Network Security review during the Fiscal Year 2012-2013, as a continuation of AMAS Project 2012-02.

The objective of the Academic Affairs Distributed Network Security, Phase I review was to assess whether network security procedures implemented within select Academic Affairs divisions, schools and administrative units were adequate to ensure the confidentiality, integrity and availability of essential or restricted information system resources and data. Phase I consisted obtained a detailed understanding of network security practices by collecting responses to a Computer Environment Internal Control Questionnaire from a sample of 12 IS support units within the following Academic Affairs divisions:

- Arts & Humanities,
- Biological Sciences,
- Jacobs School of Engineering (JSOE),
- Office of the Executive Vice Chancellor (EVC),
- Physical Sciences,
- Rady School of Management, and
- Social Sciences.

Based on the responses received from the Computer Environment Internal Control Questionnaire, AMAS performed a preliminary risk assessment to identify IS security practices within individual Academic Affairs departments for additional focused testing as part of this Phase II.

II. Audit Objective, Scope, and Procedures

The objective of our review was to further assess the adequacy of specific IS security practices within select Academic Affairs IS support units, as identified during Phase I. In order to achieve our objectives we completed the following:

- Completed network vulnerability scans using the Beyondtrust® Retina Network Security Scanner on workstations and/or servers maintained in the following Academic Affairs divisions or departments:
    - History,
    - Philosophy[1],
    - Biological Sciences,
    - The Executive Vice Chancellor's Office,
    - Rady School of Management,

[1] IS security personnel within the Jacobs School of Engineering maintain a single server for the Division of Arts & Humanities that is used by the Department of History, Department of Philosophy and the Dean's Office.

    - Chemistry & Biochemistry, and
    - Linguistics;
- For servers and/or workstations that were shown to have high risk network vulnerabilities, either verified that the vulnerability was a false-positive, or rescanned the systems after the vulnerabilities were believed to be effectively remediated;
- Completed sensitive data scanning using the Cornell Spider sensitive data scanning tool on select workstations within the Department of Music and the Rady School of Management;
- Manually reviewed the contents of a database maintained by the Department of Chemistry & Biochemistry to determine if sensitive information was effectively purged or encrypted;
- Reviewed firewall and/or switch level access control lists (ACLs) maintained in Division of Biological Sciences and the Department of Chemistry & Biochemistry;
- Reviewed and evaluated application level controls maintained over a MS Access database used by the Office of Students with Disabilities (OSD); and
- Completed a web application vulnerability scan using the Hewlett-Packard WebInspect tool on a web application internally developed and maintained by a Social Sciences department.

III. Conclusion

We concluded that the IS security controls tested were generally adequate to ensure the confidentiality, integrity and availability of data and systems within each respective Academic Affairs divisions or department. However, we did identify critical vulnerabilities on a web application developed and maintained by a Social Sciences department. These vulnerabilities had not been remediated or mitigated as of the date of this review.

In addition, network vulnerability scans identified high risk vulnerabilities on servers maintained by one Academic Affairs division that were not patched as of the date of this report.

IV. Observations and Management Corrective Actions

A. Web Application Security

An essential and sensitive web application internally developed and maintained by a Social Sciences department was found to contain critical vulnerabilities.

Many campus departments develop web applications to support a wide variety of different business and academic processes. Some of these internally developed web applications are considered essential to a department in that if there is a loss of confidentiality, availability or integrity of the application or underlying database, one or more business processes could be significantly impacted.

Another consideration is the sensitivity of the underlying data that is used or processed by a web application. Web developers must be especially careful to develop secure applications that use or handle electronic protected health information (ePHI), personal identity information (PII), or student academic records.

During the review, AMAS completed a web application vulnerability scan on a web application that was developed and maintained by a department in the Division of Social Sciences. Based on information provided by the application developer, the web application is highly utilized by staff, faculty and staff, and processes sensitive academic information. The web application vulnerability scan identified two critical vulnerabilities that had not been remediated as of the date of the review. The details of the web application and critical vulnerabilities identified by the scan have been provided to department management under separate cover.

<u>Management Corrective Action:</u>

The web application developer and Assistant Dean have been made aware of the result of the scan, and have agreed to remediate the critical vulnerabilities in a timely manner.

B. Network Vulnerabilities

One Academic Affairs division administered servers that contained vulnerabilities at the operating system level that were not patched as of the date of this report.

One of the primary risks to protection of IS systems and data is for system vulnerabilities to be exploited. In order to reduce the risk that a vulnerability will be exploited, IS security personnel frequently update and patch operating systems, and limit the number of services that are running on a device to those that are necessary. Limiting the number of services that run on a device also decreases the number of open ports on network devices, thereby reducing the risk that future vulnerabilities will be exploited.

UCSD Minimum Standards include policies related to limiting the services that are running, and for addressing vulnerabilities. Section 2.4 requires that devices only run services necessary for the intended purpose of the device. Section 6.2.3, which is applicable to only servers that participate in sensitive activities, requires that patches be applied within a week of availability. Section 6.2.5, which is a phase three requirement that must be implemented by January 1, 2009, requires that departments use a single server to support a single purpose, as to limit the number of services running on servers.

Workstations and servers in seven different Academic Affairs divisions or departments were scanned using the Beyondtrust® Retina Network Security Scanner. The purpose of the scan was to identify existing vulnerabilities on servers and workstations at the operating system and application levels. The results of the Retina server scans were provided to the responsible IS administrators under separate cover.

Most of the divisions or departments that were scanned using Retina appeared to have high risk vulnerabilities on at least one server and/or workstation. Most departments successfully patched the vulnerabilities in a timely manner, or demonstrated that scan reported false positives. However, servers in one division contained high risk vulnerabilities that were not successfully patched as of the date of this report.

Management Corrective Action:

IS administrators will evaluate the results of the Retina scans and address all high risk vulnerabilities that are not deemed false positives. AMAS will re-scan servers as needed to ensure that vulnerabilities identified in the initial scans have been addressed.