SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

July 2, 2010

CHARLOTTE KLOCK
Executive Director of Infrastructure
Interim Chief Information Security and Privacy Officer
Administrative Computing and Telecommunications
0903

Subject: ***Campus Wireless Network Upgrade – Post Implementation Review***
Audit & Management Advisory Services Project 2010-12

The final audit report for the Campus Wireless Network Upgrade, Audit & Management Advisory Services project number 2010-12, is attached. We would like to thank all members of ACT for their cooperation and assistance during the audit.

Because we were able to reach agreement regarding corrective actions to be taken in response to the audit recommendations, a formal response to the report is not requested. The findings included in this report will be added to our follow-up system. We will contact you at the appropriate time to ascertain the status of implementation.

UC wide policy requires that all draft audit reports, both hard copy and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return any remaining draft documents to mail code 0919 or destroy them at this time.

Please call me if you have any questions regarding the attached report.

Stephanie Burke
Assistant Vice Chancellor
Audit & Management Advisory Services

Attachment

cc: E. Deere
G. Lawrence
D. Larson
J. Madden
D. McLaughlin
G. Matthews
V. Polichar
E. Strahm
S. Relyea
S. Vacca

AUDIT & MANAGEMENT ADVISORY SERVICES

Campus Wireless Network Upgrade
Post Implementation Review
May, 2010

Performed By:

Daren Kinser, Auditor
Jennifer McDonald, Auditor
David Meier, Manager

Approved By:

Stephanie Burke, Assistant Vice Chancellor

Project Number: 2010-12

Table of Contents

Campus Wireless Network Upgrade – Post Implementation Review
Audit & Management Advisory Services Project 2010-12

I. Background

Audit & Management Advisory Services (AMAS) has completed a review of campus oversight for the wireless network upgrade as a component of the annual audit plan for Fiscal Year 2009-2010. This report summarizes the results of our review.

In 2009, Administrative Computing and Telecommunications (ACT) completed the installation of a state-of-the-art 802.11n wireless network with Wi-Fi protected access enterprise (WPA-E) encryption technology in all campus buildings and many public areas. The campus wireless network is centrally managed by ACT including installation and repair, helpdesk functions, data communications monitoring, and network security. The wireless network is capable of providing bandwidth of up to 200 mega bits per second (Mbps) to wireless users, depending on the tuning of their application and their proximity to a wireless access point. The upgrade replaced a 2.4 GHz coverage scheme that emphasized connectivity over security and performance.

The primary responsibility for wireless network security is provided by the security group in ACT. Secondary responsibility resides with managers of particular sections of the network (department network administrators) who are responsible for maintaining security for certain network sections. Tertiary responsibility resides with end-users who are expected to observe campus policy and best practices for computer and data security.

The campus wireless network is designed to provide three types of connectivity for end users: full access for faculty, staff and students (UCSD-PROTECTED); limited access for visitors and guests (UCSD-GUEST); and special device connectivity for network devices that are unable to configure WPA-E encryption and require static address assignments (UCSD-GUEST with no network restrictions). The UCSD-PROTECTED service uses encryption with WPA-E technology and requires an Active Directory (AD) username and password in order to authenticate. UCSD-GUEST is an unencrypted service requiring daily user registration and is restricted to basic network services such as general web browsing, printing, instant messaging, secure email, and the use of the Virtual Private Network (VPN) protocol to allow access to restricted and sensitive network resources. Campus devices that cannot do WPA2-E encryption or authentication are allowed to connect to the network after they have registered their devices with ACT, providing specific information regarding the device. This type of connection was mainly designed for wireless devices such as cameras, sensors, refrigerators, and other devices that require specialized access. These devices are allowed to use the network without authentication, encryption, and network restriction.

ACT manages security for the wireless network as one piece of an overall layered IT security strategy. Because wireless activity is ubiquitous, and wireless data traffic ultimately enters the wired network¸ ACT security resources and measures for mitigating potentially malicious activity are focused primarily on the wired environment.

II. Audit Objective, Scope, and Procedures

The objective of our review was to conduct a post-implementation assessment of the recent upgrade to the campus wireless network with an emphasis on security and project management aspects of the upgrade. The scope of the review included the new wireless network hardware, authentication and encryption mechanisms, the status of the decommissioning of legacy hardware and software, and the use of project management software for project documentation. The scope of our risk-based review also included the overall state of wireless network security including ACT security practices related to wireless network activity. Some of these practices were not substantially changed during the network upgrade. Consequently, the scope of our review also included some ACT practices that existed prior to the wireless network upgrade.

In order to achieve our objectives we completed the following:

- Conducted interviews with key personnel within ACT to gain an understanding of the wireless network deployment, maintenance, monitoring and security processes;
- Reviewed supporting technical documentation for the wireless equipment;
- Reviewed campus policies and procedures regarding network connectivity;
- Reviewed technical software applications that supported the project implementation (Source Forge) and wireless system control processes (Wireless Control System);
- Reviewed the special device connectivity process for areas of risk;
- Performed an onsite assessment for rogue access points and traffic monitoring at the Cancer Center, Biomedical Sciences Building, and Price Center;
- Performed validation procedures on results from the above assessment; and
- Reviewed wireless software patch management processes.

III. Conclusion

We concluded that the wireless network upgrade was implemented as planned to support better campus coverage, increased speed, enhanced data security via encryption, and streamlined services for visitors and guests. However, we noted some concerns in areas of deployment and operational processes that were not the result of the wireless upgrade, such as: rogue access point management; special device assessment; network access control (NAC) processes; wireless post deployment assessment; and policies and procedures. Issues of concern and opportunities for improvement are noted in detail in the balance of this report.

IV. Observations and Management Corrective Actions

A. Wireless Access Point (AP) Management – Rogue Detection

ACT had not implemented strong controls for remediating rogue AP's and addressing rogue activity.

ACT used the Wireless Control System (WCS) to monitor and manage AP activity. WCS is a software application that provides comprehensive deployment, monitoring, troubleshooting, and report generation on indoor and outdoor wireless networks. AP's are devices that allow computer users to connect to a wireless network using standard wireless protocols. ACT Installation and Repair used a monitoring feature within WCS to view information for unclassified rogue AP's.[1] An unclassified AP was defined as neither malicious nor friendly but required investigation to determine which category the AP belonged in. In order to appropriately identify an AP within WCS, the definition of a rogue AP should be further defined. During interviews of ACT personnel, we noted that the definition of a rogue AP was not comprehensively understood.

During audit fieldwork, we conducted an on-site assessment of wireless access points at Cancer Center, Biomedical Sciences Building (BSB) and Price Center. The method used at all three locations consisted of walking the floors of each building while using Kismet, an 802.11, layer2 wireless network detector, sniffer, and intrusion detection system. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, de-cloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic. The results of our assessment are as follows:

1. <u>Basic Sciences Building (BSB)</u>
   AMAS completed a walkthrough of all floors of BSB and found 308 devices, 17 of which we classified as rogue. Nine of the 17 rogues were also identified within WCS; six were not found in WCS; one was classified as friendly; one was in WCS but removed in April 2010 and reappeared with the Kismet assessment. Additional information obtained from Kismet showed 12 devices with no encryption configured and two configured with the Wired Equivalent Privacy (WEP) protocol.

2. <u>Cancer Center</u>
   All floors of the Cancer Center were scanned for wireless AP's. One rogue was identified without encryption configured, and it was not found in WCS.

[1] ACT advised that, while the Cisco WCS is a robust tool that can be used to detect the presence and location of rogue devices, rogue detection was neither its primary role nor original objective in the upgrade.

3. Price Center
   All floors of the Price Center were scanned. Nine rogue devices were identified. One device was not listed in WCS, and eight were listed in WCS and Kismet. Three devices were configured with WEP; five had no encryption configured and one appeared to use WPA.

Because rogue wireless AP's appear to be pervasive and may not require users to authenticate or encrypt wireless transmissions, sensitive information included in wireless transmissions from the locations discussed above could be inappropriately accessed, resulting in possible data security violations.

Management Corrective Actions:

ACT management will document a risk-based strategy for further classifying and remediating rogue access points and ensure that established campus wireless security standards are consistently implemented. This strategy will continue to focus on rogue activity masquerading as legitimate UCSD services as a higher risk, and radio interference as a moderate risk.

B. Unsecured Wireless Network Access – Special Devices

The process for granting unauthenticated, unencrypted access to the wireless network for special devices was not adequately controlled.

In October 2009, ACT announced a network connection process for devices that could not use the secure encryption protocols, WPA-E or WPA2-E. Users were instructed to register their devices with the UCSD hostmaster and provide the comment that the device was unable to use WPA-E/802.1x. An email confirmation from the hostmaster indicated that the user was now authorized to use the UCSD-Guest wireless network without authentication and network restriction. The process used to register special devices was based on a wireless registration form that relied on preset data fields for information to determine proper network assignment as well as email correspondences to determine relevance. It was observed that the registration page did not contain a data field requesting information regarding sensitive data. As a result, the database of devices contained missing and misidentified information, posing an unknown risk to data security.

AMAS reviewed a listing of machines that were allowed to associate as special devices. At the completion of audit fieldwork, there were a total of 469 devices using unrestricted network access. Multiple devices included on the listing did

not have complete logistic information or comments describing the type of device and why it could not be configured for WPA-E, even though the operating system listed may have been the type capable of enhanced encryption. A small sample of devices from the list was selected for review. Several entries contained user email addresses that were not listed in Blink, as well as one client hardware address found in WCS that was identified as a rogue device.

Prior to the transition to encrypted wireless, ACT received hundreds of requests for the device wireless access. In order to accommodate the requests during a small time frame the analysis activity for each device was postponed to a later date. ACT is in the process of a three-phased approach for assessing the current list of devices allowed to connect without authentication or encryption.

Management Corrective Actions:

- ACT will complete a comprehensive audit of current device access to determine need, and create a procedure to properly analyze devices before allowing future connection to the network; and

- ACT will modify the registration form to gather information regarding the type of data that will be traversing between the wireless network and the connecting device. This information will be used to identify high risk machines as well as assess the need for access.

C. Network Access Control

Clients were allowed access to the wireless network without a detailed security assessment, creating the risk of possible security vulnerabilities.

Security assessments for clients connecting to the campus wireless network consisted of security scans looking for critical vulnerabilities after the client had connected to the network. A pre-assessment was not in place for host security controls such as: ensuring active host firewalls were implemented, operation system patches were up to date, and active antivirus and spyware application were installed.

Network Access Control (NAC) is a computer networking solution that uses a set of protocols to define and implement policies describing how clients obtain secure access to network resources as they initially attempt to connect to the network. This process includes policies such as pre-admission endpoint security checks and post-admission controls over what resources users may access. It can also integrate an automatic remediation process to ensure the information system is operating securely before network association is allowed to occur.

At the time of our review, staff interviews indicated that a project to design and develop a pre-security assessment for wireless clients was in the initial concept phase but was not currently on an active project plan. Due to the fact that the wireless network does not receive the same level of comprehensive scanning as the general campus network, there is a moderate security risk associated with allowing non-compliant hosts to connect to the network.

Management Corrective Action:

ACT management will reassess the project priorities for development of a NAC solution to allow for active security assessment of hosts attaching to the wireless network.

D. Source Forge (SF) Post Assessment - Wireless Deployment

A post implementation assessment for wireless project management activities had not occurred, possibly resulting in undetermined risks to security and business processes due to inter-dependent activities not being identified and fully addressed.

SF is a web-based repository that provides a centralized location to control and manage open source software development. It provides access to data storage and tools for managing projects, and is best known for providing a revision control system. The ACT Information Technology (IT) Applications division implemented SF in June of 2009 as a tool for managing Software Development Lifecycle (SDLC) projects, as well as managing other project activities within ACT such as infrastructure enhancements. The intent was to use the 22 steps identified within a project lifecycle and incorporate adjustments to the actual activities within in each step for the type of project being managed. ACT IT Infrastructure implemented the use of SF for tracking tasks and document retention during the wireless deployment. SF was implemented after the upgrade to the UCSD-Protected network. An alternate web-based system was used as a document repository and as containment for tasks, timelines and campus notifications.

AMAS reviewed the task listing and documents within SF and observed that post implementation plans and activities were not conducted or documented completely. A project is considered complete when it has been successfully implemented and transitioned to the operational unit and approved by management. Responsibilities may include assessing how closely the project met user needs, identifying what worked well, learning from mistakes made during the

project, identifying patterns and trends, constructing ways to improve the processes used throughout the project, and communicating results.
The purpose of conducting a Post-Implementation Review is to gather the information required to meet those responsibilities, and to present the information in a Post-Implementation Report so that interdependent activities are properly addressed, resourced and completed. Ideally, post-implementation assessments which indicate that high risk issues remain to be addressed would be fully documented in SF through their ultimate resolution. The status of rogue AP management practices and unauthenticated devices noted above appear to be such issues.

Management Corrective Actions:

- The Manager of ACT Infrastructure and Outreach has indicated that all projects moving forward are now using the prescribed project management framework for tracking status, resources, and documenting activities and completion as applicable.

- The Manager of ACT Infrastructure and Outreach will review the project management tasks used for the wireless implementation and compare them to the structured project management design process within Source Forge. This information will be used to improve ACT IT Infrastructure processes as appropriate.

E. Policies, Procedures, and Communications

Standards and administrative procedures for wireless connectivity were not specifically referenced in the UCSD Policy and Procedure Manual (PPM) 135-3 titled *Network Security.*

During audit interviews, ACT personnel described the wireless network standards that were used to manage the UCSD campus wireless network, referencing PPM 135-3 and Blink. The wireless overview on Blink described connection standards in a manner that appeared to read like a policy directive although Blink is considered more an informal repository of information.

At the time of this review, PPM 135-3 defined UCSD campus user and department responsibilities for protection of campus network information assets. However, the policy did not include wireless technical system standards including deployment configurations, authentication requirements, data encryption requirements, the access authorization process and validation of installations per standards. Because the policies are generally written to address issues at an institutional level, it would be reasonable for ACT to develop and document

technical and network administration standards in support of the wireless network as well as correlating and supporting the detailed information provided in Blink. In addition, raising awareness to wireless security issues on a regular basis through campus communication will assist in addressing security concerns with regards to rogue AP's and special device access. These measures will provide ACT with the policy directive and authority to actively monitor and remediate rogue activity, and enforce the use of enhanced encryption standards for wireless connectivity. Documented standards and procedures help to ensure process consistency and continuity.

Management Corrective Actions:

- ACT management will review and update PPM 135-3 to include specific language governing wireless devices, connections and security; and

- ACT will communicate policy changes to the campus community prior to remediation and enforcement activities.