SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

January 23, 2012

TODD PAWLICKI
Director, Radiation Oncology Clinical Operations
0843

CASEY SANDACK
Chief Business Officer, Radiation Oncology
0843

Subject: ***Cancer Center Data Security – Phase II, Radiation Oncology***
Audit Project 2012-26C

The final audit report for Cancer Center Data Security – Phase II, Radiation Oncology; Audit Report 2012-26C, is attached. We would like to thank you and your Information Technology team for the cooperation and assistance we received 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 agreed upon time to evaluate the status of the corrective actions. At that time, we may need to perform additional audit procedures to validate that actions have been taken prior to closing the audit findings.

UC wide policy requires that all draft audit reports, both printed and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS personnel, or destroy them. AMAS also requests that draft reports not be photocopied or otherwise redistributed.

Stephanie Burke
Assistant Vice Chancellor
Audit & Management Advisory Services

Attachment

cc: E. Babakanian
D. Brenner
M. Collins
R. Fletcher
G. Matthews
T. McAfee
A. Mundt
T. Perez
C. Wenger
K. Wottge
S. Vacca

AUDIT & MANAGEMENT ADVISORY SERVICES

University of California
San Diego

Cancer Center Data Security – Phase II
Radiation Oncology
January 2012

Performed By:

Daren Kinser, Auditor
Jennifer McDonald, Auditor
Terri Buchanan, Manager

Approved By:

Stephanie Burke, Assistant Vice Chancellor

Project Number: 2012-26C

Cancer Center Data Security – Phase II
Radiation Oncology
Audit & Management Advisory Services Project 2012-26C

Table of Contents

Executive Summary

Audit & Management Advisory Services (AMAS) has completed a review of the data security processes and technologies implemented by Radiation Oncology (RO) to manage the network that supports all treatments and administrative matters in the department. The department consists of approximately 30 servers and 175 workstations.

The Radiation Oncology (RO) network connects to the UCSD campus backbone network, and is managed by a Computer Resource Manager and a Programmer Analyst (RO IT), in coordination with campus Administrative Computing and Telecommunications (ACT) and UCSD Health System Information Services personnel. It consists of approximately 30 servers and 175 workstations. In contrast to applications supported on a general business network, the RO IT network provides Radiation Oncologists with the specialized healthcare applications and medical equipment interfaces necessary to perform a wide range of radiation therapy treatments. As a result, much of the data that is processed by and stored on the RO network is highly sensitive personally identifiable information (PII) or protected health information (PHI). The maintenance of a robust network security infrastructure is critical to protect against damage to systems or data, which would impact RO's ability to control radiation treatment devices, facilitate other patient services, and ensure compliance with Federal and State laws, and University policies.

Based on the preliminary risk assessment performed, the objectives of our review were to determine whether processes and technologies implemented to secure Information Technology (IT) resources, and the sensitive data stored on RO clinical workstations and file servers were adequate to minimize the risk of unauthorized access or data loss; and to validate that standard security measures implemented were functioning as designed.

Based on our review procedures, we concluded that network security practices appeared generally adequate to ensure the confidentiality, integrity and availability of essential or restricted information system resources and data. However, we identified two areas of risk involving systems and application security on servers and workstations. In addition, we noted some areas where activities were not in strict compliance with policy requirements including minimum standards; risk assessment activities; and information security planning.

In response to the audit findings, RO management will implement the following corrective actions:

- Address all high and medium risk vulnerabilities not deemed to be false positives identified in the Retina scans; close all ports not needed to support business operations; and move printers that are addressed in public IP space to private IP space.
- Implement Minimum Standards required logging parameters for servers and client machines; perform periodic scans on servers and workstations to identify and secure unencrypted sensitive data; and update the host registration information to provide complete and accurate data for all RO devices.
- Complete a comprehensive risk assessment to identify primary security objectives for protecting information resources, and develop an information security plan based on those results.

I. Background

Audit & Management Advisory Services (AMAS) has completed a review of the data security processes and technologies implemented by Radiation Oncology to manage the network that supports its Encinitas and Moores Cancer Center operations. This report provides the results of our review.

The Moores Cancer Center (MCC) is one of five UCSD School of Medicine (SOM) Organized Research Units (ORUs). Established in 1979, the MCC is one of 40 National Cancer Institute (NCI) designated Comprehensive Cancer Centers in the United States. MCC research laboratories and clinic facilities support clinical and non-clinical cancer related research projects, cancer prevention and outreach programs, and comprehensive clinical care.

The Radiation Oncology (RO) network connects to the UCSD campus backbone network, and is managed by a Computer Resource Manager and a Programmer Analyst (RO IT), in coordination with campus Administrative Computing and Telecommunications (ACT) and UCSD Health System Information Services personnel. It consists of approximately 30 servers and 175 workstations. In contrast to applications supported on a general business network, the RO IT network provides Radiation Oncologists with the specialized healthcare applications and medical equipment interfaces necessary to perform a wide range of radiation therapy treatments. As a result, much of the data that is processed by and stored on the RO network is highly sensitive personally identifiable information (PII) or protected health information (PHI). The maintenance of a robust network security infrastructure is critical to protect against damage to systems or data, which would impact RO's ability to control radiation treatment devices, facilitate other patient services, and ensure compliance with Federal and State laws, and University policies.

Departments that manage sensitive data must be focused on ensuring that network security is adequate to comply with applicable regulations. PII is subject to the provisions of California State Bill 1386. Systems that store PHI are subject to Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements.

In addition to legislative requirements, RO computer equipment must also conform to University of California (UC) Business and Finance Bulletin IS-3 (IS3), *Electronic Information and Security Policy;* and UCSD Policy and Procedure Manual 135-3 (PPM 135-3), *Network Security*; and PPM 135-3 Exhibit C: *Minimum Network Connection Standards* (Minimum Standards). IS3 establishes guidelines for achieving appropriate protection for University electronic resources and identifying roles and responsibilities at all levels in the University of California system. PPM 153-3 Exhibit C standards provide minimal security requirements for devices that are connected to the UCSD Campus network backbone.

In May 2011, AMAS completed a preliminary network security risk assessment of the RO network based on elements of IS3, PPM 135-3 and the Minimum Standards. The risk assessment results were compiled using information obtained through analyzing responses to a Computer Environment Internal Control Questionnaire (ICQ) and supporting documentation, and conducting follow-up interviews with RO IT. Based on those procedures, we determined that a focused review should be performed for selected areas to verify that certain network security controls were in place and performing as expected.

II. Audit Objectives, Scope, and Procedures

Based on the preliminary risk assessment performed, the objectives of our review were to determine whether processes and technologies implemented to secure Information Technology (IT) resources, and the sensitive data stored on RO clinical workstations and file servers were adequate to minimize the risk of unauthorized access or data loss; and to validate that standard security measures implemented were functioning as designed.

We completed the following audit procedures to achieve project objectives:

- Reviewed PPM135-3, Minimum Standards, and IS3;
- Interviewed the RO Computer Resource Manager and Programmer Analyst to further assess areas of risk;
- Analyzed the Access Control Lists (ACL's) that restrict network data traffic to and from RO networked resources (workstations and servers);
- Evaluated host-based firewall rules that control incoming and outgoing data traffic to workstations and servers;
- Assessed work station and server configurations logging requirements and host registration information;
- Reviewed vendor contracts and Business Associate Agreements (BAA) for RO patient care systems;
- Performed network vulnerability scanning using Retina on selected RO file servers and workstations, and evaluated reported vulnerabilities; and,
- Completed an information security review based on elements of IS3, PPM 135-3 and the Minimum Standards (***Attachment A***).

Some RO network devices used in direct patient care including, printers, scanners, routers, firewalls and switches were excluded from vulnerability scans to ensure that patient services were not disrupted.

At the time of this review, RO managed the operation of two satellite facilities, one in Encinitas and the second in South Bay. The South Bay facility was not evaluated within the scope of this review.

III. Conclusion

Based on our review procedures, we concluded that network security practices appeared generally adequate to ensure the confidentiality, integrity and availability of essential or restricted information system resources and data. However, we identified two areas of risk involving systems and application security on servers and workstations. In addition, we noted some areas where activities were not in strict compliance with policy requirements including minimum standards; risk assessment activities; and information security planning.

The details of these findings are discussed in the remainder of this report.

IV. Observations and Management Corrective Actions

A. Systems and Application Security

Vulnerability scans completed on RO network servers and workstations identified system vulnerabilities, and a number of open ports on network devices.

One of the primary risks to network hardware and data is the potential exploitation of system vulnerabilities[1]. In order to reduce the risk that a vulnerability will be exploited, IS security personnel frequently apply updates and patches to software, and limit the number of services that are running on a device to only those that are necessary to achieve business objectives. 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 several policies related to limiting the number and type of device services that are running, and addressing system 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 only to servers that process sensitive information, requires that patches be applied within a week of availability. Section 6.2.5, which was to be implemented by January 1, 2009, requires that departments use a single server to support a single purpose, and to limit the number of services running on servers.

[1] A system vulnerability is a weakness which allows an attacker to reduce a system's information assurance. A vulnerability reflects the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

AMAS completed network vulnerability scans on computing devices administered by RO IT using the Retina Network Security Scanner to identify existing vulnerabilities, and ports that were open on servers and workstations. Separate scans were completed for devices located in Encinitas and La Jolla RO facilities. Credentialed and non-credentialed scans were performed on selected servers and workstations at both locations. Credentialed scanning allows a detailed view of software patch levels, and high level system configurations. Non-Credentialed scanning provides the same view of the network that is seen by an individual without network permissions. The results of the Retina scans were provided to RO IT personnel under separate cover.

The scans identified a number of vulnerabilities on department servers in both locations; and three of those servers contained sensitive information. In addition, the network scans identified open ports on the majority of department servers and workstations. Some of the open ports were running unknown services, which should be reviewed to determine their business use, and to verify that malicious software such as rootkits[2], and Trojans[3] are not installed. These types of programs have typically been used to launch denial of service attacks, to launch further attacks against other campus systems, and to facilitate the sharing of inappropriate data. All unnecessary services should be identified and stopped, and any associated ports should be blocked.

A small number of what appeared to be printers in the public internet protocol (IP) address space were discovered in the scan results. Minimum Standards 4.1 state that printers, network scanners and faxes, and other network appliances must be deployed in private IP spaced when possible.

Management Corrective Actions:

RO IT will:

1. Evaluate the results of the Retina scans and address all high and medium risk vulnerabilities that are not deemed to be false positives.

2. Review open port lists, and close all ports that are not necessary to support business operations.

3. Move the printers that are addressed in public IP space to private IP space.

[2] A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications.

[3] A Trojan horse, or Trojan, is software that appears to perform a desirable function for the user prior to run or install, but which, sometimes in addition to the expected function, steals information or harms the system.

B. Minimum Standards Compliance

RO was not in strict compliance with Minimum Standards with regard to system audit logging, scanning for sensitive data, and IP host registration.

The UCSD Minimum Standards were implemented to reduce the risk that UCSD computing equipment and data are compromised. Computing equipment configurations or IT management processes that do not meet Minimum Standards represent a significant potential security threat, which could result in substantial mitigation costs if security breaches occur.

1. Audit Logging

Most components of an IT infrastructure are capable of producing logs to capture their activity over time. The logs often contain very detailed information about the activities of applications and the layers of software and hardware that support them. With proper management, device activity logs can enhance security, system performance and resource management when used to perform the following functions:

- Monitor access controls;
- Reconstruct security incidents; and
- Achieve regulatory compliance.

Minimum Standards for workstations and servers that process and manage sensitive information require that logs be generated that identify the user, type of event, date and time with time zone, success or failure and origin of event, and the system component, and affected data, or resource. During our review, we noted that RO had some logging parameters enabled for servers that process sensitive information. However, the complete logging configuration required by Minimum Standards was not defined.

Management Corrective Action:

RO IT will fully implement the logging parameters for servers and client machines that process sensitive information required by the Minimum Standards.

2. Scanning for Sensitive Data

Minimum Standards for workstations and servers that process and manage sensitive information require departments to scan their systems to identify unencrypted sensitive data at least monthly. Minimum Standards further state that, sensitive data should be removed from the system when possible. If it cannot be removed, sensitive data must be encrypted. During our review, we noted that RO IT had not implemented a process to continually address unencrypted sensitive data, which increases the potential of security threats to RO resources.

<u>Management Corrective Action:</u>

RO IT will research available software, and develop a process to perform periodic scans on servers and workstations to identify and secure unencrypted sensitive data.

3. <u>IP Host Registration</u>

Minimum Standards for workstations and servers that connect to the campus data communications network require that all devices be registered with ACT via the UCSD Hostmaster. In addition, registration information must be periodically reviewed and updated as needed. In July 2010, ACT modified the host registration form to gather information regarding the type of data that will be hosted on the connecting device. This information is used to identify high risk machines as well as assess the need for access.

AMAS evaluated a small judgmental sample of RO devices and noted that several servers that stored PHI were not registered with the UCSD Hostmaster. For all registered devices we reviewed, the registration did not list the sensitive data stored on the device.

<u>Management Corrective Action:</u>

RO IT will review and update the host registration information to provide complete and accurate data for all RO devices.

C. Risk Assessment

RO IT would benefit from a comprehensive risk assessment to identify and classify information assets and identify potential risks.

The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. Departments or units that manage information assets and electronic resources should conduct formal risk assessments to determine the level of protection needed to adequately protect various existing information resources, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. As business operations, workflow, or technologies change, periodic reviews should be conducted to analyze these changes, to account for new threats and vulnerabilities created by these changes, and to determine the effectiveness of existing controls.

UCOP provides general guidelines for developing a risk assessment, which include:

- Identify assets covered by the assessment
- Categorize potential losses
- Identify threats and vulnerabilities
- Identify existing controls
- Analyze the data
- Determine cost-effective safeguards
- Report to Management

During the review, we noted that RO did not employ a comprehensive risk assessment process. RO IT was able to provide detailed information regarding the systems that they managed; however, specific risks and a level of security necessary to protect those resources were not identified and formally documented.

Management Corrective Action:

RO IT and Management will perform a comprehensive risk assessment to identify primary security objectives for protecting information resources. The risk assessment will include classification of the information assets stored on the devices or within the applications and identify the level of security necessary to protect the information resources. Additional Risk Assessment resources are included in ***Attachment B***.

D. Information Security Plan

RO IT would benefit from a documented security plan to enhance the security of information assets.

An information security plan should be developed that takes into consideration the acceptable level of risk for systems and processes. A security plan should account for the management, use, and protection of confidential information; and identify the procedures and controls that are needed to enhance security for information assets. It should also identify cost-effective strategies to be implemented to mitigate the risks that are consistent with organizational goals and business functions. The security plan should be developed at the completion of the risk assessment process. Because RO IT had not performed a comprehensive risk assessment, the security plan to consider acceptable risk levels and proper mitigation was not in place.

<u>Management Corrective Action:</u>

RO IT and Management will develop an information security plan that identifies acceptable level of risk for information assets, systems and processes.

Cancer Center Data Security – Phase II
Radiation Oncology
Audit & Management Advisory Services Project 2012-26C
Information Security Review - Attachment A

Assessment Categories	Objective	Risk Assessment
Management Measures: People		
1. Security Education and Awareness Training	Assess employee's awareness of System-wide Security policies.	No Reportable Observations
Technical Measures		
2. Identity and Access Management	Assess the technical measures for controlling authentication and authorization (password policy, access rights/roles).	No Reportable Observations
3. Access Controls to Authenticate and Authorize Users	Assess the controls for session protection, automatic logout, and procedures for managing privileged accounts.	No Reportable Observations
4. Systems and Application Security	Assess the procedures in place for systems responsibilities including separation of duties; backup and retention efforts; and patch management practices.	**See Report Observation A**
5. Application Systems Management	Assess the process for application version control and migration practices from development to quality assurance to the production environment. Assess the change management practices for software development and configuration.	No Reportable Observations
6. Collection, Management and Analysis of Log Data	Assess the audit log infrastructure and review practices.	No Reportable Observations
7. Data Protection and Encryption	Assess the use of encryption for data in transit and data at rest.	No Reportable Observations
8. Risk Mitigation Measures	Assess the process for prevention, detection, and recovery from emergency conditions.	No Reportable Observations
9. Network Security Tools and Practices	Assess the network security strategies and technical security measures (Minimum Standards for Network Connectivity).	**See Report Observation B**

Assessment Categories	Objective	Risk Assessment
Management Measures: Processes		
10. Asset Inventory and Classification	Assess the process for identifying electronic information resources.	No Reportable Observations
11. Risk Assessment	Assess the process to understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources. Identify the level of security necessary for the protection of the resources	**See Report Observation C**
12. Information Security Plan	Assess the departments documented process for accepting a level of risk for systems and processes, and that procedures and controls in place will enhance the security of information assets.	**See Report Observation D**
13. Workforce Administration	Assess the protection for granting and/or revoking authorizing and protecting access to information systems.	No Reportable Observations
14. Physical/Environmental Controls	Assess the procedures for physical protection of resources that support restricted or essential systems and/or data.	No Reportable Observations
15. Incident Response Planning and Notification Procedures	Assess the process for reporting and handling a security incident	No Reportable Observations

Cancer Center Data Security – Phase II
Radiation Oncology
Audit & Management Advisory Services Project 2012-26C
Risk Assessment Guidelines - Attachment B

Risk Assessment Methodology Overview [1]

Many different approaches to risk assessment have been developed. These following guidelines provide a simple step-by-step process. Additional resources and methodologies are linked under Resources to help you establish an approach appropriate to your business environment.

General Guidelines for a Risk Assessment

1. **Establish the risk assessment team**. The risk assessment team will be responsible for the collection, analysis, and reporting of the assessment results to management. It is important that all aspects of the activity work flow be represented on the team, including human resources, administrative processes, automated systems, and physical security.
2. **Set the scope of the project.** The assessment team should identify at the outset the objective of the assessment project, department, or functional area to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be reviewed, and operations to be observed.
3. **Identify assets covered by the assessment**. Assets may include, but are not limited to, personnel, hardware, software, data (including classification of sensitivity and criticality), facilities, and current controls that safeguard those assets. It is key to identify all assets associated with the assessment project determined in the scope.
4. **Categorize potential losses**. Identify the losses that could result from any type of damage to an asset. Losses may result from physical damage, denial of service, modification, unauthorized access, or disclosure. Losses may be intangible, such as the loss of the organizations' credibility.
5. **Identify threats and vulnerabilities**. A threat is an event, process, activity, or action that exploits a vulnerability to attack an asset. Include natural threats, accidental threats, human accidental threats, and human malicious threats. These could include power failure, biological contamination or hazardous chemical spills, acts of nature, or hardware/software failure, data destruction or loss of integrity, sabotage, or theft or vandalism. A vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be identified by addressing the following in your data collection process: physical security, environment, system security, communications security, personnel security, plans, policies, procedures, management, support, etc.
6. **Identify existing controls**. Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.
7. **Analyze the data**. In this phase, all the collected information will be used to determine the actual risks to the assets under consideration. A technique to analyze data includes preparing a list

[1] Risk Assessment Methodology gathered from UCOP website

of assets and showing corresponding threats, type of loss, and vulnerability. Analysis of this data should include an assessment of the possible frequency of the potential loss.

8. **Determine cost-effective safeguards**. Include in this assessment the implementation cost of the safeguard, the annual cost to operate the safeguard, and the life cycle of the safeguard.
9. **Report**. The type of report to make depends on the audience to whom it is submitted. Typically, a simple report that is easy to read, and supported by detailed analysis, is more easily understood by individuals who may not be familiar with your organization. The report should include findings; a list of assets, threats, and vulnerabilities; a risk determination, recommended safeguards, and a cost benefit analysis.

Additional Resources:

Departmental Security Review and Planning

http://www.ucop.edu/irc/itsec/securityreview.html

BFB IS-2 Inventory, Classification, and Release of University Electronic Information

http://www.ucop.edu/ucophome/policies/bfb/is2.pdf

Risk Assessment Resources

http://www.ucop.edu/irc/itsec/riskresources.html