UTHealth
The University of Texas
Health Science Center at Houston

Office of Auditing & Advisory Services

July 10, 2015

Report on Exchange System Audit #15-206

We have completed our audit of the Microsoft Exchange Server system. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

Microsoft Exchange Server

The Microsoft Exchange Server (Exchange) provides calendar, email, contact management, instant messaging, and other collaboration/work flow functionality. Sensitive data such as student/patient records, schedules, and financial information move across email and other components of Exchange. Two versions of Exchange (Exchange 2010 for Data Center Operations & Support Services and Exchange 2013 for SBMI) are currently utilized by UTHealth.

Due to the extensive amounts of email that is transferred throughout UTHealth on a daily basis, limits have been placed on the amount of email each user has available on the server. For students, faculty, and staff, the mailbox size is limited to 2GB (no limit for SBMI). Internal attachments are restricted to 75MB (100MB for SBMI) and external attachments are restricted to 50MB. Any attachments exceeding these amounts are blocked and dropped from the server. Several attachment types are automatically blocked to limit the spread of viruses across UTHealth.

Proofpoint

As hackers are constantly changing tactics and developing more sophisticated strategies, organizations are in need of full lifecycle protection against various threats. UTHealth utilizes Proofpoint, an application that provides a secure e-mail gateway with sophisticated dynamic malware analysis, real-time threat intelligence, and automated threat responses. This application allows UTHealth to more effectively detect and block targeted attacks, then quickly respond when a potential compromise has been detected.

The University of Texas Systemwide Policy 165 (UTS 165)

UTS 165 requires that each faculty member, staff, and student exercise prudence in the use of electronic communications and use them in accordance with each entity's policies, standards, and/or procedures related to information resources. Additionally, all entities are required to implement technical safeguards (based on risk) to adequately protect the security of sensitive digital data during electronic communications and transmissions. Further, UTS 165 requires that user accounts be reviewed, removed, and/or disabled at least annually, or more often if warranted by risk.

HOOP 175 - ***Roles and Responsibilities for University Information Resources*** **(HOOP 175)**
HOOP 175 requires the safeguarding of University information resources against threats that can reduce or eliminate data availability, compromise integrity, and violate confidentiality. All individual users are responsible for their use, management, and protection of information resources and are accountable for their actions.

HOOP 180 - ***Acceptable Use of University Information Resources*** **(HOOP 180)**
HOOP 180 requires that University information resources be used appropriately to ensure their availability and preserve their integrity and confidentiality so the University can meet its academic, research, and clinical commitments and goals. Users must not use their University email account to send e-mail that is likely to contain computer viruses, "chain letter" email, or "broadcast" email (unsolicited to large groups). Users are cautioned to exercise due diligence when communicating information about the University to non-users through electronic means such as email, text messages, and chat rooms. HOOP 180 also designates email addresses as the property of the University and requires that University business be conducted using University email accounts (not personal or non-University email accounts) and that confidential information in email must be encrypted.

ITPOL-005 ***Change Management Policy*** **(ITPOL-005)**
ITPOL-005 requires changes to production data and programs be made only by authorized parties at the approved time according to established procedures. Significant changes must use a change notification procedure in accordance with ITSOP-005 *Change Notification Procedure*.

ITSOP-005 ***Change Notification Procedure*** **(ITSOP-005)**
ITSOP-005 requires that changes to information resources be made only after appropriate documentation, review and coordination, and that they are communicated and managed in a prudent and consistent manner so that other IT support staff and the user community can plan accordingly. Change notifications are entered into the Change Notification System and include information such as the change description, pre-production testing and results (if applicable), the urgency of the change, risk level, and validation results expected. The Change Management Oversight Team consists of IT members representing the following areas: Academic Technology, Administrative Technology, Clinical Technology, Communication Services, Data Center Operations and Services, Desktop Services, IT Compliance, IT Security, Medical School, and the School of Public Health. The Change Oversight Management Team conducts a review of all change notifications on a periodic basis and monitors various change metrics.

Exchange Server Security Guides
Microsoft publishes an Exchange Server Security Guide for each Exchange system product, which is designed to inform administrators about features that may affect security considerations. Typical features discussed include the admin center, architecture, data loss prevention, rights management, anti-malware protection, managing recipients, sharing and collaboration, high availability, and workload management. Auditing and Advisory Services (A&AS) reviewed and considered the Exchange Server Security Guides during the course of our audit procedures.

OBJECTIVES

The objective of this audit is to determine whether the controls around Exchange configuration and delivery are adequate to ensure the availability and protection of information resources.

SCOPE AND METHODOLOGY

Through a review of UTHealth policies and procedures, consideration of Security Guides, interviews with IT personnel and control owners, a review of user access and configuration, and testing of preventative/detective controls around external threats, Auditing and Advisory Services (A&AS) performed an audit of the Exchange system.

AUDIT RESULTS

User Access

A&AS interviewed key personnel at the Data Center Operations and Support Services group (DCOS), the School of Biomedical Informatics, and Legal Affairs to gain an understanding of the processes for maintaining and implementing user access associated with the Exchange system and related components, including Proofpoint and the Rand Secure Archive System.

A&AS compared the list of systems administrators and privileged users to their respective job descriptions and determined that assigned roles and responsibilities were appropriate.

Additionally, A&AS reviewed the access listings for the Exchange system and the related components. For the Proofpoint application, we noted that a regular review of access is not performed and a previously terminated system administrator still maintained access.

Recommendation 1:
We recommend that a process be implemented for reviewing Proofpoint access on a periodic basis. Additionally, the access for the previously terminated system administrator should be revoked.

Management's Response: Instead of implementing a separate process for periodically reviewing terminated employees, the Proofpoint application will be reconfigured to use directory authentication. This will allow for the automatic removal of access based on the current PeopleSoft employment status of each individual assigned access.

Responsible Party: Kevin Granhold
Implementation Date: November 30, 2015

Server Configuration & Updates

A&AS interviewed various IT personnel in order to gain an understanding of the operating and system architecture for the Exchange system. DCOS utilizes Windows 2008 for the operating system and Exchange 2010 for the email server, while SBMI utilizes Windows 2012 and Microsoft Exchange 2013, respectively. We obtained the Microsoft Support Lifecycle Information and verified that all operating systems are currently supported by the vendor.

Using the Baseline Security Analyzer tool, we requested that DCOS run a comparison between the configurations of the Exchange servers to the recommended security and configuration guides. Based on the comparison results, it was determined that security setting for Internet Explorer (for one administrator) is not consistent with the recommended setting per the Best Practices Analyzer tool.

Recommendation 2:
We recommend that the security setting for the administrator be changed to the recommended setting per the Baseline Security Analyzer tool and that DCOS perform a periodic audit of the Exchange server configuration using the Baseline Security Analyzer tool.

Management's Response: The Baseline Security Analyzer tool for the Exchange Operating System will be run during each server patching cycle, or four times per year. The results will be carefully examined to determine if the recommendations should be implemented as stated, modified, or not implemented at all. This decision will be based on risk, productivity, value and the severity of the issue being addressed. We will document the reasons for not implementing recommendations.

Responsible Party: Kevin Granhold
Implementation Date: November 30, 2015.

There were no add-on software updates made to the DCOS Exchange servers during the audit period. Proofpoint was upgraded from version 7.2 to 8.0 on June 11, 2015. A testing environment was not available to conduct pre-production review and testing prior to the upgrade as required by ITSOP-005.

Recommendation 3:
As Proofpoint is critical in protecting Exchange, we recommend IT secure a test environment with the vendor in order to conduct pre-production reviews and testing prior to future Proofpoint upgrades.

Management's Response: We agree with the recommendation and will secure a test environment.

Responsible Party: Kevin Granhold
Implementation Date: November 30, 2015

A&AS obtained and reviewed the change management policies and procedures and noted that while they apply to the entire UTHealth enterprise, SBMI does not currently follow ITPOL-005 or ITSOP-005, nor have they developed internal change management policies and procedures. Additionally, SBMI was not involved in the recent upgrade of Proofpoint.

Recommendation 4:
We recommend that SBMI follow ITPOL-005 and ITSOP-005 (or develop equivalent policy and procedures).

Management's Response: Change requests will be categorized into those that have an impact outside of SBMI and those that only impact SBMI. For changes that have an impact outside of

SBMI, the change request will be subject to ITPOL-005 and ITSOP-005. For changes that only impact SBMI, we will develop our own change management policies and procedures and follow them.

Responsible Party: Ryan Bien and David Ha
Implementation Date: January 31, 2016

External Threats
A&AS interviewed various IT personnel in order to gain an understanding of the technical controls to protect against spam, viruses, malware, spoofing, and phishing attacks against the Exchange system. DCOS utilizes Proofpoint along with firewalls and load balancing controls for protection against external threats. For the SBMI Exchange servers, an antivirus filter package (part of the Microsoft Forefront Protection tool) is also utilized. Based on a review of system configuration documentation, the deployed tools contain up-to-date protection.

In order to assess the effectiveness of Proofpoint, A&AS obtained evidence that IT Security utilizes the Proofpoint Dashboard to monitor and review protection levels against external threats on a regular basis. We selected a judgmental sample of threats and reviewed/assessed the adequacy of the remedial and corrective actions taken. Malware and phishing incidents of a higher severity are reported to UT System on a monthly basis. No exceptions were noted.

In order to gain an understanding of the controls around the remote access of Exchange servers, A&AS interviewed DCOS personnel and determined that system administrators have the ability to remotely log in to Exchange servers using two-factor authentication though the Virtual Private Network (VPN). Remotely accessed data is protected using Secure Socket Layer (SSL) and anonymous access has been properly disabled. The technical controls around remote access to Exchange servers appear to be adequate.

A&AS interviewed IT Security and reviewed the most recent network scans of the Exchange servers. We reviewed and assessed the adequacy of the corrective actions taken as a result of the network scans. No exceptions were noted.

Protection of Sensitive Data
A&AS interviewed key personnel at DCOS, IT Security, and SBMI to gain an understanding of technical controls around the protection of sensitive data when sending unencrypted email or not using Digital IDs.

The Data Loss Prevention (DLP) features of Proofpoint are configured to detect and block outgoing email that contains sensitive data. In certain situations, it can also be configured to automatically encrypt outgoing email (containing sensitive data) before it is released.

In order to test the effectiveness of Proofpoint controls, 28 test emails with an attachment were sent to an external email address. Simulated sensitive data was included in the attachment and a variety of keywords (such as "Social Security Number", "DOB", "SSN", etc.) were added to the email header, content, and attachment title. The following issues were noted:

- For a sample of 28 test emails sent with simulated sensitive data in the attachment, Proofpoint did not identify and block 15 (54%) emails.

- Of the 28 test emails, five were sent from an email account with an active encryption license. Each of the five emails contained simulated sensitive data (including social security and credit card numbers) in the attachment. Proofpoint did not identify and self-encrypt one (20%) of the emails. A subsequent retest was performed and the self-encrypt was successful.

Recommendation 5:
We recommend that IT work with the vendor to determine whether Proofpoint can be further configured to detect and block outgoing email containing sensitive data.

Management's Response: We agree with the recommendation and the results of the discussion with Proofpoint will be documented.

Responsible Party: Kevin Granhold
Implementation Date: November 30, 2015

CONCLUSION

Controls around the Exchange configuration and delivery are generally appropriate and functioning as intended. Recommendations were made around monitoring Proofpoint access, periodically performing an audit of the Exchange configuration, utilizing a test environment for future Proofpoint upgrades, the development of change management policies and procedures for SBMI, and working with the vendor to determine if Proofpoint can be further configured to detect and block outgoing email containing sensitive data.

We would like to thank the IT, IT Security, and Legal Affairs staff and management who assisted us during our review.

Daniel G. Sherman
Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

DGS: BBS

cc: Audit Committee
Rick Miller
Amar Yousif
Arlene Staller
Kevin Granhold
Ryan Bien

Audit Manager:	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned:	Lieu Tran

Issue Date: August 17, 2015