Office of Internal Audit

UT Southwestern Medical Center

Data Security Audit – Non-Employees

Internal Audit Report 18:15

10/22/2018

Table of Contents

Executive Summary

Background

Cybersecurity breach and unauthorized data access constitutes a strategic risk for UT Southwestern Medical Center (UTSW) as its systems are under constant threat of attack or misuse of data from inside and outside the organization. Due to the increasing complexity of affiliate relationships, business partners and contractual relationships with service providers and other vendors, there is also increased risk of unauthorized access by vendors and other non-employees if the relationships and oversight of access is not properly managed. The Data Security Audit – Non-Employees was performed to evaluate the controls in place to ensure UTSW information systems and data are adequately protected against these risks due to physical and system access granted to non-employees.

UTSW departmental management is responsible for requesting access to campus facilities and information systems for the non-employees they sponsor through vendor contractual relationships, as well as timely requesting removal of access upon termination. Administrative functions involved in the access management governance and related processes include:

- Information Security with direct reporting line to the Office of the President - responsible for information security policies, standards and procedures.
- Human Resources:
  - Employee Relations from within the Office of Human Resources - responsible for employee separation policies.
  - Human Resources Information Systems (HRIS) - produces and distributes to departmental personnel contacts a monthly report of active employees and non-employees (the “Active Employee Listing (AEL) Report”).
- Systems Access Management (SAM) reporting to Information Resources - responsible for maintaining access to the UTSW network.
- Access Control reporting to the Chief of Police, University Police - responsible for issuing badges and maintaining physical access to UTSW facilities.

The PeopleSoft Human Capital Management (HCM) system is used to manage the employment status of non-employees, known as types: Person of Interest (POI) or Contingent Workers (CWR). Data interfaces from HCM to Microsoft Active Directory via Microsoft Identity Manager, as well as the Lenel badge access control system, assist in automating certain aspects of network and physical access management including removal upon termination.

Scope and Objectives

The Office of Internal Audit has completed its Data Security audit. This was a risk based audit and part of the fiscal year 2018 Audit Plan. The audit scope focused on the management of access granted to vendors and affiliates. The scope period was from the beginning of fiscal year 2018 to current. Audit procedures included interviews with stakeholders, review of policies and procedures and other documentation, substantive testing, and data analytics.

Executive Summary

The overall objectives for the Data Security Audit were to review the processes and controls in place to ensure compliance with policies and procedures, adequate oversight and monitoring procedures exist for ensuring appropriateness of data access for affiliates, vendors, and other Person of Interest (POI) types. Control objectives reviewed included:

- Access is disabled timely when no longer needed.
- Responsible departmental managers monitor active status of vendors or contingent workers.
- Responsible departmental managers are identified and receive communication to validate and recertify security access for vendor and contingent worker status.
- Non-employee badge access is deactivated promptly upon termination of relationship with UTSW.
- Expected end date for non-employee accounts are synchronized between HCM and their network accounts.
- Responsible departmental managers periodically recertify user access to critical systems.

We conducted our examination according to guidelines set forth by the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Conclusion

Overall, opportunities exist to improve vendor relationship management processes, specifically, monitoring of compliance with Human Resources and Information Security policies and procedures to ensure physical and system access for non-employees is removed timely. Monitoring is needed to detect retroactive entry of termination transactions as well as compliance with the monthly active employee and non-employee certification requirements. Escalation and reporting should be done when department management is not following policy, given the significant risk of inappropriate access. Finally, automated processes to remove physical access upon termination can be improved.

Included in the table below is a summary of the observations noted, along with the respective disposition of these observations within the Medical Center internal audit risk definition and classification process. See Appendix A for Risk Rating Classifications and Definitions.

Priority (0)	High (1)	Medium (2)	Low (0)	Total (3)

Strengths identified during the audit include:

- Through a system interface, network accounts are automatically deactivated upon termination of position assignment in PeopleSoft HCM.
- With the implementation of PeopleSoft version 9.2, the Expected End Date field is now required for all POIs, facilitating the termination process.

Executive Summary

The improvement opportunities included in this report are summarized below:

- **#1 Implement monitoring and revise relevant policies to ensure timely termination of non-employees –** Termination transactions are not always entered timely at the department level to the PeopleSoft HCM system when non-employees terminate, increasing the risk of unauthorized access.
- **#2 Coordinate and monitor terminations to ensure prompt deactivation of access badges when termination becomes effective –** Physical access badges are not always timely deactivated when non-employees terminate, which may result in unauthorized physical access to UT Southwestern facilities.
- **#3 Implement monitoring and reporting procedures for ensuring department management validation of active employees –** Monitoring and reporting procedures are not in place at the department level to ensure department administrators comply with the procedure to monthly certify their active employee and non-employee accounts are reported on the Active Employee List (AEL).

Management has plans to address the issues identified in the report and in some cases, have already implemented corrective actions. These responses, along with additional details for the improvement opportunities listed above are listed in the Detailed Observations and Action Plans Matrix (Matrix) section of this report.

We would like to take the opportunity to thank the departments and individuals included in this audit for the courtesies extended to us and for their cooperation during our review.

Sincerely,

Valla F. Wilson, Associate Vice President for Internal Audit, Chief Audit Executive

Executive Summary

Audit Team:
Gabriel Samuel, Senior IT Auditor
Jeff Kromer, Director, IT & Specialty Audit Services

cc: Irfan Butt, Assistant Vice President, Systems and Operations
Ed Donoho, Supervisor Access Control Technical Operations, University Police
Arnim E. Dontes, Executive Vice President, Business Affairs
Kenneth Kellough, Assistant Vice President, Budget and Resource Planning
Sharon Leary, Assistant Vice President, Accounting and Fiscal Services
Jodi Levy, Assistant Vice President, Administrative Systems
Marcus Lewis, Chief of Police, University Police
Marc E. Milstein, Vice President, Information Resources & Chief Information Officer
Heather Mishra, Associate Vice President, Academic & Administration Information Systems
Darren Nelson, Assistant Vice President, Human Resources Administration
Wade Radicioni, Director of Operations and Analytics, Academic Affairs
Joel Reyes, Manager, Human Resources Information Systems
Mary Robles, Manager, IR Systems Access Management
Michael Serber, Vice President, Finance and Institutional Chief Financial Officer
Julie Sirkin, Assistant Vice President, Compensation, Benefits and Human Resource Information Systems (HRIS)
Cameron Slocum, Vice President and Chief Operating Officer, Academic Affairs
Joshua Spencer, Associate Vice President and Chief Information Security Officer
Thomas Spencer, Ph.D., Assistant Vice President, IR Operations and Compliance, Academic and Administrative Information Resources
Dwain Thiele, M.D., Interim Executive Vice President, Academic Affairs & Provost/Dean, UT Southwestern Medical School
John Warner, M.D., MBA Executive Vice President Health System Affairs & Chief Executive Officer, University Hospitals

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: High n 1. **Implement Monitoring and Revise Relevant Policies to Ensure Timely Termination of Non-Employees** Termination transactions are not always entered timely at the department level in the PeopleSoft HCM system when non-employees terminate, increasing the risk of unauthorized system access and data loss. Testing revealed 92 termination transactions for non-employees entered from one to 50 days late during FY2018. This is primarily the result of the lack of reporting, monitoring and escalation processes to establish accountability and enforce policy compliance In addition, there is no Human Resources policy to address non-employee termination and Information Resources policy ISR-111 System Access Management is missing requirements, which would improve accountability, including: · A deadline for system administrators to remove access granted to terminated non-employees. · A deadline more specific than "as soon as practicable" for sponsors or managers of non-employees to request removal of access after termination.	1. Implement reporting, monitoring and escalation processes for late entry of termination transactions to enforce compliance with Information Security Policy ISR-111, and escalate repeat offenders for disciplinary action as deemed necessary. 2. Develop and offer refresher compliance training targeted at managers, sponsors and department administrators responsible for entering termination transactions in HCM to equip them with adequate knowledge of the requirements and expectations for prompt termination of employees and non-employees. 3. Develop a policy to require department administrators to enter termination transactions within two business days for consistency with policy ISR-111. 4. Revise Policy ISR-111 to provide: · A deadline for system administrators to remove access granted a user upon termination. · A defined timeline for managers and sponsors to request termination of system access for non-employees upon termination. This should be consistent with the two-day limit currently stated in the policy for entry of termination transactions in HCM.	**Management Action Plans:** 1. Information Security will work with the associated departments to identify measures which could be used to detect untimely entry of termination transactions. These measures will be evaluated by executive management to determine which controls are warranted and the appropriate timeline for implementation. **Action Plan Owners:** Associate Vice President & Chief Information Security Officer Assistant Vice President, Administrative Systems **Target Completion Dates:** December 31, 2018 2. AAIR Operations Training will coordinate with Information Security to develop supporting training materials as recommended and schedule for completion 30 days after the design of the process specified in #1.1 is completed. **Action Plan Owners:** Assistant Vice President, IR Operations and Compliance **Target Completion Dates:** January 31, 2019

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
		3. A policy will be developed to require department administrators to enter termination transactions within two business days of termination. **Action Plan Owners:** Assistant Vice President, HR Administration **Target Completion Dates:** December 31, 2018 4. Defined timelines will be added to policy ISR-111 as recommended stating “as soon as practicable, but not to exceed two business days unless authorized by the Chief Information Security Officer.” **Action Plan Owners:** Associate Vice President & Chief Information Security Officer **Target Completion Dates:** November 30, 2018

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium n 2. **Coordinate and Monitor Terminations to Ensure Prompt Deactivation of Access Badges When Termination Becomes Effective** Physical access badges are not always being timely deactivated when employees and non-employees terminate, which may result in unauthorized access to facilities and subsequent unauthorized system access. An interface from the PeopleSoft Human Capital Management (HCM) system to the Lenel Access Control system automatically deactivates badges upon termination. However, procedures are not in place to manually intervene to deactivate badges when there is an error or downtime occurs in the interface. Comparison of active badges to PeopleSoft HCM employee and non-employee records and Active Directory network account records identified nine the employees and non-employees whose badges remained active after their termination date. While access badges are generally collected and shredded upon termination as a compensating control, one of the badges was not collected and was used 30 days past the termination date.	1. Ensure procedures for deactivating terminated employee badges include monitoring and manual intervention for instances of errors or downtime in the automated interface to ensure badges are deactivated timely upon termination. 2. Evaluate the effort and specifications necessary to customize HCM to require the Expected End Date to be required for Contingent Workers (CWR), as is currently required for POIs, to prevent the risk of unauthorized access when departments don't enter termination transactions timely. 3. Until HCM is updated to have the required end date for CWRs, implement system reporting and monitoring procedures to identify incidents of terminated accounts with active badges or Expected End Date has passed.	**Management Action Plans:** 1. Procedures for monitoring and manually deactivating badges when errors or downtime occur in the interface have been implemented. The protocol for immediate error resolution will be that IR will email Badge Access Control to ask for a badge to be activated or deactivated, depending on the situation. **Action Plan Owners:** Chief of Police, University Police Assistant Vice President, Administrative Systems **Target Completion Dates:** Completed 2. We agree an expected end date should be required in HCM for CWRs and we will implement such customization in HCM. As with POIs this customization will include a default maximum of one year with variable lengths for specified job codes. We will coordinate with the Provost's Office to define exceptions for certain faculty-related job codes not requiring a date. **Action Plan Owners:** Assistant Vice President, Human Resources Administration Assistant Vice President, Compensation, Employee Benefits, HRIS Assistant Vice President, Administrative Systems

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
		Target Completion Dates: December 31, 2018 3. We will coordinate with IR to develop monthly reporting of employees and non-employees who have terminated or whose expected end date has passed and review a random sample to verify the badges have been deactivated. **Action Plan Owners:** Chief of Police, University Police Assistant Vice President, Administrative Systems **Target Completion Dates:** December 31, 2018

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium n 3. **Implement Robust Procedures for Ensuring Department Management Validation of Active Employees** Monitoring and reporting procedures at the department level are not in place to ensure procedures are followed. Department administrators are not always complying with the procedure to monthly certify their active employees and non-employees reported on the Active Employee List (AEL). The rate of responses for compliance with the certification procedure as recorded on the HRIS web site is generally low, ranging from 15-30% since April 2018 when the AEL email messaging was last revised. Per feedback from a sample of recipients, they feel this low response rate is due to the content and structure of the email not being clear and the link to the HRIS web site not being prominent.: In addition, the following process deficiencies were noted: · No follow up email is sent to remind recipients to respond. · Responsibility for monitoring compliance with the certification procedure has not been designated. · Procedures for escalating instances of non-compliance are not in place.	1. Evaluate the feasibility of developing a solution to automate the AEL reporting and certification functionality on a single page, similar to the SharePoint-based solution used for Epic user access re-certification. 2. Designate a function and leader responsible for monitoring the response rate reports for compliance, implement processes to send reminders and escalate instances of non-compliance for further review and disciplinary action as deemed necessary. 3. As an alternative in the event a new solution as recommended in #3.1 above is not feasible, redesign the look and content of the AEL email to make it more concise. Improve recognition of the certification hyperlink by separating it from the text and consider displaying in uppercase letters to further reinforce compliance. Also include requirements to (1) obtain monthly reports from vendors regarding the active status of non-employees working remotely, and (2) update the Expected End Dates for POIs where this date is not specified in HCM. Finally, rename the AEL report attachments to clearly represent their content.	**Management Action Plans:** 1. We will evaluate the feasibility of the following options for implementation and present to the EVP of Business Affairs for consideration and approval to move forward: a. Coordinate with Accounting and Fiscal Services and the Budget Office to include a separate paragraph for Employee/CWR/POI attestation in distribution of the monthly department financials reports with attestations directed to HR. b. Coordinate with IR to develop a customized program for recording and reporting of department attestation. Monitoring and escalation of instances of non-compliance would then be performed by Human Resources. **Action Plan Owners:** Assistant Vice President, Human Resources Administration Assistant Vice President, Compensation, Employee Benefits, HRIS Manager, Human Resources Information Systems Assistant Vice President, Administrative Systems **Target Completion Dates:** December 31, 2018

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
		2. Functional responsibility for monitoring and escalation will be assumed by HR after implementation of the option chosen in #3.1 above. **Action Plan Owners:** Assistant Vice President, Human Resources Administration Assistant Vice President, Compensation, Employee Benefits, HRIS Manager, Human Resources Information Systems **Target Completion Dates:** December 31, 2018 3. The Office of Human Resources will do the following: a. Until an automated solution can be implemented as noted in #3.1 above, redesign the content of the AEL email to make it more concise and rename the AEL reports to clearly represent their content by November 30, 2018. b. Work with the departments and IR (HCM team) to evaluate the best method and then populate an expected end date for CWRs without an end date.

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
		Action Plan Owners: Assistant Vice President, Human Resources Administration Assistant Vice President, Compensation, Employee Benefits, HRIS Manager, Human Resources Information Systems Assistant Vice President, Administrative Systems **Target Completion Dates:** a. November 30, 2018 b. January 31, 2019

Appendix A – Risk Classifications and Definitions

As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our review. The following chart is intended to provide information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

	Degree of Risk and Priority of Action	
Risk Definition- The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	**Priority**	An issue identified by Internal Audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.
	High	A finding identified by Internal Audit that is considered to have a high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	Medium	A finding identified by Internal Audit that is considered to have a medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action is needed by management in order to address the noted concern and reduce the risk to a more desirable level.
	Low	A finding identified by Internal Audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action should be taken by management to address the noted concern and reduce risks to the organization.

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the subsequent pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions. It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.