17-207 Data Loss Prevention (Digital Guardian)

We have completed our audit of Digital Guardian. 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

As follow-up to a prior audit finding involving cloud computing, IT Security implemented a combination of firewall content filtering and data loss prevention (DLP) controls to detect and respond to inappropriate storage of sensitive data in consumer cloud sites. The Digital Guardian (DG) application was selected and implemented as the DLP solution. DG assists with the classification of data and provides the capability to detect and prevent the egress of protected data to cloud storage and file sharing sites. DG can also log the egress of protected data to portable drives, storage media, and printers.

Content classification (detection of names and social security numbers) for newly created/copied files was recently disabled on clinical workstations with DG installed due to performance issues, which are currently being investigated. This risk is somewhat mitigated by the fact that Allscripts and other clinical electronic health records are accessed through Citrix servers and the downloading of patient records is limited.

OBJECTIVES

The objective of this audit was to determine whether controls around data loss prevention and the Digital Guardian (DG) application are adequate and functioning as intended.

SCOPE PERIOD

The scope period was January 1, 2017 to September 15, 2017.

METHODOLOGY

The following procedures were performed:

- Selected a sample of clinical workstations and those with access to the Claims Database Environment (CDE) and verified DG agents were properly installed.
- For designated higher risk (Context) applications, verified application is properly tagged in the DG application and names/social security numbers are included in classification tables.
- For a sample of non-Context applications, generated a dummy test file and moved it to a variety of external locations. Verified DG monitoring and notification controls are operating effectively.

713.500.3160 phone
713.500.3170 fax
P.O. Box 20036
Houston, Texas 77225
www.uthouston.edu

- Selected a sample of DG alerts and obtained evidence of communication to LAN managers, IT management, and others where appropriate. Verified alerts were properly actioned/resolved.

AUDIT RESULTS

A&AS identified areas of improvement related to policy and procedures, managing DG inventory, and configuring the DG application:

- There are no formal policies and procedures around the DG application and tracking/resolution of alerts.
- A number of workstations with access to sensitive data did not have DG installed. Additionally, there is no inventory list of all workstations with DG agents installed.
- Periodic verification of tagging by Context applications is not performed.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None

We would like to thank the staff and management within IT Security, Medical School Information Technology, and Clinical Information Technology who assisted us during our review.

Brook Syers, CPA, CIA, CFE, CISA
Senior Audit Manager, I.T.

MAPPING TO FY 2017 RISK ASSESSMENT

Risk (Rating)	R.12 Sensitive UTHealth data is stored on unsanctioned cloud storage providers (Critical) R.26 Sensitive UTHealth data stored on vendor cloud is not secure (High)

DATA ANALYTICS UTILIZED

Data Analytic #1	None

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Audit Manager	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned	Lieu Tran, CISA
End of Fieldwork Date	December 1, 2017
Issue Date	December 20, 2017

Copies to:
Audit Committee
Amar Yousif
Rick Miller
Dr. Ryan Walsh
Dr. James Griffiths
Bassel Choucair
Ryan Bien

17-207 Data Loss Prevention (Digital Guardian)

Issue #1	Section G of *HOOP-175 Roles and Responsibilities for University Information Resources and University Data* requires the Chief Information Security Officer to develop, oversee the implementation of, and monitor a documented Information Security Program and related security policies and procedures. A&AS noted there are no formal policies and procedures around data loss prevention, the DG application, and the tracking/resolution of alerts generated by DG.
Recommendation #1	We recommend IT Security develop and implement formal policies and procedures around data loss prevention, the Digital Guardian application, and the tracking/resolution of alerts generated by Digital Guardian.
Rating	Medium
Management Response	IT Security will add language to the existing Computer Security Incident Response Policy to address security incidents related to data loss prevention. IT Security will also create an internal standard operating procedures document detailing the steps that need to be taken for Digital Guardian alerts.
Responsible Party	Amar Yousif, CISO
Implementation Date	June 18, 2018

Issue #2	Section 3.2 of *UTS165 Information Resources Use and Security Policy* states the Security Program must include and document a current inventory of mission-critical applications and applications containing confidential data. Further, Section 10.1 requires each institution to maintain an accurate inventory of information resources and identify owners. A&AS selected a random sample of five UT Physicians clinics and one research area, conducted an onsite visit, and selected a sample of 28 on-site workstations to verify DG was installed. Of these 28 workstations, 4 (14%) did not have DG installed. Additionally, we noted there is no inventory list of all workstations with DG agents installed.
Recommendation #2	We recommend MSIT and SBMI Desktop Services develop a process to ensure all applicable workstations have DG agents installed and are properly inventoried and tracked.
Rating	Medium

Management Response #2a	MSIT will develop a checklist showing that Digital Guardian is to be installed prior to any clinical system being deployed to an end user. MSIT will utilize System Center Configuration Manager (SCCM) to identify UTP end points that do not have Digital Guardian installed and will remediate them by installing and verifying the installation on identified systems.
Responsible Party	Bassel Choucair, Executive Director, Information Technology, McGovern Medical School
Implementation Date	August 31, 2018

Management Response #2b	SBMI IT has requested that the CDE access be revoked for the SBMI user workstation identified in the finding. Additionally, we will update our policy to require the installation of DG agents on the primary workstations of researchers who have access to the CDE.
Responsible Party	Ryan Bien, Associate Dean For Management II, SBMI
Implementation Date	January 31, 2018

Issue #3	DG has been configured by IT Security to detect the downloading of files from Context applications. Files downloaded from designated applications are "tagged" by DG and, if they are subsequently moved/transferred, DG will provide a warning to the user, deliver email notifications to the IT Security inbox, generate alerts to IT Security/Local Area Network Managers/DG Administrators, and record events in the DG event log, or all of the above. During our walkthrough of a Context application at the School of Public Health, A&AS noted a downloaded file was not properly tagged by DG. We verified the tagging issue was remediated during fieldwork.
Recommendation #3	We recommend IT Security periodically verify Context applications are properly tagging downloaded files.
Rating	Medium
Management Response	IT Security will explore ways to automate periodic health checks for profiled applications. Until automation is completed, IT Security will manually perform health checks every six months, or after every major application change, to verify that Digital Guardian is properly profiling applications.
Responsible Party	Amar Yousif, CISO
Implementation Date	June 18, 2018