Secretary of State
Oregon Audits Division

Department of Administrative Services and Enterprise Information Services

Recommendation Follow-up Report: Security at the Data Center Continues to Improve, but More Work Remains to Address Weaknesses

April 2020
Report 2020-16

Secretary of State Bev Clarno
Audits Division Director Kip Memmott

Follow-up to Audit Report 2018-34

Department of Administrative Services
Enterprise Information Services

Recommendation Follow-up Report: Security at the Data Center Continues to Improve, but More Work Remains to Address Weaknesses

April 2020

Follow-up Summary

Enterprise Information Services (EIS), formerly the Office of the State Chief Information Officer, made progress on nine of the 11 recommendations from the original audit, fully implementing two. However, additional work remains to clearly define security management roles and to improve security capabilities at the data center.

Findings from the Original Audit

- EIS has made significant progress in improving security at the data center, though progress is needed to refine these processes and better track vulnerability remediation.
- Some security areas require improvement, including privileged access, asset and configuration management, and security incident response.
- Day-to-day computing remains stable and disaster recovery capabilities have improved, but the data center needs to work with its customers to prioritize which systems should be recovered first in the event of disaster.

Improvements Noted

- Funding has been approved for equipment lifecycle replacement at the data center, (pg. 4) including one-time funding for an automated information technology service management solution. (pg. 5)
- Processes are in place to track security event volume and content (pg. 3) and potential incidents. (pg. 5)

Remaining Areas of Concern

- Security management roles are not clearly articulated. (pg. 3)
- No controls are in place to isolate unsupported operating system environments. (pg. 4)
- Privileged access membership and user activity monitoring need improvement. (pg. 4-5)

The Oregon Secretary of State Audits Division is an independent, nonpartisan organization that conducts audits based on objective, reliable information to help state government operate more efficiently and effectively. The summary above should be considered in connection with a careful review of the full report.

Introduction

The purpose of this report is to follow up on the recommendations we made to Enterprise Information Services (EIS) as included in audit report 2018-34, "Progress Has Been Made to Address Security Weaknesses at the State Data Center, but Improvements Are Still Needed."

The Oregon Audits Division conducts follow-up procedures for each of our performance audits. This process helps assess the impact of our audit work, promotes accountability and transparency within state government, and ensures audit recommendations are implemented and related risks mitigated to the greatest extent possible.

We use a standard set of procedures for these engagements that includes gathering evidence and assessing the efforts of the auditee to implement our recommendations; concluding and reporting on those efforts; and employing a rigorous quality assurance process to ensure our conclusions are accurate. We determine implementation status based on an assessment of evidence rather than self-reported information. This follow-up is not an audit, but a status check on the agency's actions.

To ensure the timeliness of this effort, the division asks all auditees to provide a timeframe for implementing the recommendations in our audit reports. We use this timeframe to schedule and execute our follow-up procedures.

Our follow-up procedures evaluate the status of each recommendation and assign it one of the following categories:

- **Implemented/Resolved**: The auditee has fully implemented the recommendation or otherwise taken the appropriate action to resolve the issue identified by the audit.
- **Partially implemented**: The auditee has begun taking action on the recommendation, but has not fully implemented it. In some cases, this simply means the auditee needs more time to fully implement the recommendation. However, it may also mean the auditee believes it has taken sufficient action to address the issue and does not plan to pursue further action on that recommendation.
- **Not implemented**: The auditee has taken no action on the recommendation. This could mean the auditee still plans to implement the recommendation and simply has not yet taken action; it could also mean the auditee has declined to take the action identified by the recommendation and may pursue other action, or the auditee disagreed with the initial recommendation.

The status of each recommendation and full results of our follow-up work are detailed in the following pages.

We sincerely appreciate the courtesies and cooperation extended by officials and employees of EIS during the course of this follow-up work.

Relevant divisions have changed their names since the audit

Since our original audit, the auditee and several of its divisions have been renamed. The Office of the State Chief Information Officer is now Enterprise Information Services, or EIS. The Enterprise Security Office, a division of EIS, is now Cyber Security Services (CSS). Finally, Enterprise Technology Services, also a division of EIS, is now Data Center Services (DCS).

Despite these name changes, the organizational structure of EIS remains the same. EIS, an organizational unit of the Department of Administrative Services (DAS), is led by the State Chief Information Officer who reports directly to the Governor. EIS is responsible for providing centralized computer services for state agencies through DCS. CSS is responsible for centralized enterprise cybersecurity for state agencies. Together, DCS and CSS ensure the security of information technology assets at the state data center.

Recommendation Implementation Status

Recommendation #1

Clarify the information security roles of data center personnel pertaining to security requirements defined in the information security plan and overall responsibility for security at the data center.	**Partially implemented**

CSS management worked with a consultant to draft a document clarifying cybersecurity roles and responsibilities among CSS, DCS, state agencies, and other entities. However, we noted that the draft document does not clearly articulate security incident response roles and responsibilities between the various parties. As management moves forward with finalizing this document, it is important that they ensure all security roles are clearly defined.

CSS management indicated that they hope to finalize and share this document with DCS and other agencies in March 2020, though this timeline is dependent on external stakeholders.

DCS management chose to postpone clarification of security roles specific to the data center until after CSS has finalized the document.

Recommendation #2

Improve tracking of remediation efforts to mitigate critical vulnerabilities detected by scans.	**Implemented**

Management implemented an interim solution to address this recommendation. Agency personnel track the top 10 critical vulnerabilities identified in monthly reports in a ticket tracking information system. While this is an improvement of the agency's processes to track remediation, DCS could further improve this process by tracking critical vulnerabilities beyond the top 10.

Ultimately, data center management plans to leverage the information technology service management (ITSM) system discussed in recommendation no. 10 as a more efficient and automated solution. However, work is still underway to identify and implement this system.

Recommendation #3

Improve implementation and capabilities of the security information and event monitoring system by: a. developing metrics to measure and track volume and content of logs and associated offenses generated by the system; b. developing procedures to modify system rules; and c. continuing to build capacity to manage additional log sources for input and analysis of the system.	**Partially implemented**

CSS implemented processes to measure and track the volume and content of logs, which are reported weekly to internal management, fully satisfying part "a" of this recommendation.

Management has developed a procedure governing the modification of rules to the system. However, the procedure does not address key change management controls, such as how changes will be reviewed and documented. This part of the recommendation has been partially satisfied.

CSS implemented new hardware to provide additional capacity for the security information and event monitoring system to manage input and analysis of information from additional log

sources, fully satisfying part "c" of this recommendation. Considering actions taken on all three parts, we rate this recommendation as partially implemented.

Recommendation #4

Request funding from the Legislature to implement networking and security equipment lifecycle replacement as an ongoing program as opposed to individual projects.	**Implemented**

DAS requested funding for equipment lifecycle replacement and software licensing upgrades and tool replacement at the state data center during the 2019 legislative session. The Legislature approved the request. While the amount of funding will likely change each biennium due to growth and cost variations, this provides an avenue to request ongoing funding for lifecycle replacement needs at the data center.

Recommendation #5

Develop and implement solutions to isolate operating system environments that are not fully supported by vendors.	**Not implemented**

DCS has not yet developed solutions to isolate unsupported operating system environments. Management indicated that these solutions will be included in their network security modernization project. However, this project is still in the planning phase, and no documentation exists to indicate how the recommendation will be addressed by the project.

Recommendation #6

Periodically reconcile installation of anti-malware and patch management agents on Windows servers with applicable servers in its inventory to ensure full coverage.	**Partially implemented**

Management implemented a manual reconciliation process to address this recommendation. DCS personnel conducted the first review during our follow-up and management indicated they plan to perform reconciliations quarterly. This manual review is time-consuming and does not account for all discrepancies. However, if the process is refined, this review can provide a stop-gap solution to ensure that anti-malware and patch management agents are up to date.

Ultimately, data center management plans to leverage the ITSM system discussed in recommendation no. 10 as a more efficient and automated solution. However, work is still underway to identify and implement this system.

Recommendation #7

Enforce existing procedures requiring periodic review of privileged access membership.	**Partially implemented**

During our initial audit, we found DCS was not in compliance with several division policies requiring periodic privileged access account review. While some of these processes are still not occurring, management implemented a regular review of changes to privileged accounts to ensure that such changes are authorized. Though this review will help mitigate the risk that users are inappropriately granted elevated access, the process does not catch all changes.

In addition, further work remains for management to assess policies governing privileged access review, along with the review processes in place, to ensure they are aligned and adequately mitigate the risk of inappropriate privileged access membership.

Recommendation #8

Develop additional alerts to monitor actions taken by privileged access users, as required by the statewide security plan and standards.	**Not implemented**

Additional alerts to monitor actions taken by privileged access user have not yet been developed. CSS is working with a vendor to implement privileged account use monitoring in the security incident and event monitoring system; this builds on the body of work addressed in recommendation no. 3c. Once the solution is in place, management indicated that CSS and DCS will work together to implement this functionality at the data center. However, at this time, CSS does not have processes in place to monitor privileged access at the data center in accordance with state standards.

Recommendation #9

Further define procedures for security incident response, including: a. better defining roles and responsibilities for security incident response between Cyber Security Services (formerly the Enterprise Security Office) and the data center; b. ensuring that potential security incidents are tracked to enable additional analysis; and c. developing standard operating procedures for responding to different types of security incidents.	**Partially implemented**

DCS is in the process of revising its Security Incident Management Plan, which now includes a high-level flowchart of its security incident management process. CSS is also in the process of revising their Information Security Incident Response Plan. Given that this work is still in process, we consider part "a" partially satisfied. However, we noted it took some effort to decipher the division of roles and responsibilities between the two entities, which may lead to confusion during a security incident. As the divisions work to finalize these incident response documents, it may benefit CSS and DCS to work together to improve consistency and clarity.

CSS established a process to record potential incidents, detected by automated systems or other sources, in a ticket tracking system. Incident response personnel review logged items and incident handlers follow up on any that are determined to be an actual security incident. This fully satisfies part "b" of the recommendation.

CSS developed an Information Security Incident Response Procedures document. The procedure outlines steps responders should take to identify, classify, contain, eradicate, and recover from a security incident. This document, in combination with supplemental guidance referenced in the procedure, addresses how to respond to different types of security incidents. This fully satisfies part "c" of the recommendation. Considering actions taken on all three parts, we rate this recommendation as partially implemented.

Recommendation #10

Identify and implement an automated solution for asset inventory and configuration management.	**Partially implemented**

DCS has begun the work necessary to identify an automated solution for asset inventory and configuration management. The Legislature approved funding for an ITSM solution at the data center during the 2019 legislative session. The state currently has two Master Price and Services Agreements, which will include functionality for asset and configuration management. DCS plans to pursue an ITSM solution through the available price agreements; however, data center

management has additional work to do to secure a vendor, including developing a Request for Quote from the two vendors.

Recommendation #11

Work with state agencies dependent upon the data center for disaster recovery and ensure priorities for recovery are identified.	**Partially implemented**

While DCS cannot implement this recommendation on its own, it has started to work with state agencies to identify recovery priorities in the event of a disaster. However, additional outreach and coordination is needed to complete this effort. During a CIO Advisory Council meeting on August 21, 2018, data center personnel requested state agencies to provide their priorities for system recovery. Data center staff continued to follow up with agencies to request this information through emails and meetings with agency management. However, this work with the agencies to identify disaster recovery priorities has been on hold since the departure of the data center's Disaster Recovery Program Manager, a position that has been vacant since October 2019. Management has since extended an offer to a candidate who has verbally accepted and plans to start April 2020.

DCS management also indicated that, as part of an effort to test a recent power upgrade, they requested agencies submit a list of their database servers and the order in which their systems should be recovered. Management believes this will further inform their disaster recovery prioritization efforts.

Conclusion

EIS made progress in addressing our recommendations, including obtaining funding for an ongoing equipment lifecycle replacement program and one-time funding for an ITSM. Once implemented, the ITSM should improve asset and configuration management, vulnerability remediation tracking, and patch and antivirus validation. In the meantime, management chose to establish interim processes to improve vulnerability remediation tracking and to reconcile patches and antivirus agents to Windows servers.

DCS also continues to work with CSS to monitor and manage security risks. CSS tracks security events and potential incidents and recently added hardware to accommodate additional log sources for security monitoring. However, while both DCS and CSS developed documents to clarify security management and incident response roles and responsibilities, not all of these documents have been finalized.

In addition to further clarifying roles and responsibilities, additional work remains to ensure privileged access membership and activity is adequately monitored. Though management implemented a process to review privileged user accounts to ensure appropriate membership, the division has yet to implement other processes outlined in its policies. Additionally, DCS management should work with CSS to ensure processes are in place to monitor privileged access activity.

Follow-up Report Team

William Garber, CGFM, Deputy Director

Teresa Furnish, CISA, Audit Manager

Jessica Ritter, CPA, CISA, Senior Auditor

Sheila Faulkner, Staff Auditor

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

This report is intended to promote the best possible management of public resources.
Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits