

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
Tori Hunthausen,
Chief Deputy Legislative Auditor



Deputy Legislative Auditors:
James Gillett
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members
CC: Janet Kelly, Director, Department of Administration
Dick Clark, Chief Information Officer
FROM: Dale Stout, Information System Auditor
DATE: June 12, 2007
RE: Department of Administration, IS Audit Data Center Review Follow-up 07SP-025
(orig. 06DP-05)

INTRODUCTION

We presented our information system (IS) audit of the Montana Department of Administration's Data Center to the Legislative Audit Committee in June 2006. The report contains five recommendations. The recommendations relate to:

- ▶ Planning and management of the data center;
- ▶ Data center physical security;
- ▶ Data center environmental security;
- ▶ Data center recover and incident response; and,
- ▶ Priority of data center security measures.

We requested and received information from the Department of Administration (DoA) personnel regarding progress toward implementation of the report recommendations. This memorandum summarizes their response.

BACKGROUND

A data center is a facility used for housing and protecting computers and communications equipment that stores and processes data necessary to support business operations. DoA maintains a central data center as a service to state agencies. Information resources residing within the data center are critical servers, systems, and data including the Statewide Accounting, Budgeting, and Human Resources System, the Department of Revenue's IRIS System and Department of Public Health and Human Services systems.

Follow-up Discussion

The following sections summarize the report recommendations, and the department's progress towards implementing the recommendations.

Planning and Management

Planning and management of the data center sets the tone for the level of protection by understanding what equipment and systems reside in the data center, knowing where the responsibility for protection lies, knowing what controls are in place and what are lacking, and mitigating the identified threats to the extent possible.

The audit identified a lack of an updated data center inventory as well as who was responsible for maintaining that inventory. DoA also had not identified and documented threats to the data center, what threats have been addressed by controls, risks to the data center as a result of those threats or performed a cost analysis of how to address the threats.

Recommendation #1

We Recommend the Department:

- A. Maintain and update the inventory of equipment, systems and data residing in the data center.
- B. Coordinate with all agencies that have hosted systems in the data center to rank the systems' criticality and establish a priority for the order in which systems will be brought back up.
- C. Evaluate existing threats to the data center including the potential impact or harm.
- D. Conduct a cost analysis associated with implementing or improving controls.
- E. Define the responsibility for, and coordinate with agencies to utilize the existing software package to develop disaster recovery plans.

A. Recommendation Status: Partially Implemented

At the time of the audit inventories of systems and data existed but were outdated. DoA stated they would consolidate, update and maintain a data center inventory and draft a policy requiring staff to maintain inventory records as part of routine work processes. Currently DoA has an automated process in place that inventories data center equipment daily, updates a data center inventory database, produces a daily inventory spreadsheet, and compares the results to the database; any exceptions are manually posted to the database. The spreadsheet has also been compared to a list of equipment IBM provides as part of their support duties. This allows the database to be used as a basis for updating the IBM support contract. I reviewed the spreadsheets and determined they are produced daily. The data inventory is not yet updated; it will be updated as part of the state's Continuity Of Operations Planning (COOP) efforts (refer to Recommendation #4). The inventory maintenance policy has been requested of the CIO Policy Team.

B. Recommendation Status: Partially Implemented

At the time of the audit if systems in the data center were brought down, the order in which agency systems would be brought back up was unclear. DoA responded by stating they will work with agencies on COOP planning, paying particular attention to their recovery plan for agency critical systems residing in the data center. This will be completed as part of the state's COOP efforts (see Recommendation 4).

C. Recommendation Status: Implemented

At the time of the audit DoA had not identified and documented threats to the data center, determined threats that are not addressed by a control, or determined the need for controls to address an existing threat or vulnerability. DoA stated they would conduct a threat and impact assessment for the data center by participating in a Capitol complex vulnerability assessment. The assessment was conducted in the fall of 2006; I reviewed the findings and results of the assessment as it related to the data center. As a result of the vulnerability assessment, ITSD developed a data center risk assessment; however after reviewing the risk assessment I determined it focuses more on the data center audit than on the vulnerability assessment.

D. Recommendation Status: Not Implemented

The audit determined efforts to implement data center controls have been limited to damage control and remediation as problems arise rather than a formal proactive approach to determine the adequacy of the control based on risk and cost analysis. DoA stated a cost analysis would be conducted based on the results of the Capitol complex vulnerability assessment. Although a risk assessment has been prepared based on the vulnerability assessment, the cost analysis has not yet been completed. DoA represents it is in the process of evaluating the risk assessment; no final approval date has been determined.

E. Recommendation Status: Partially Implemented

Disaster and Emergency Services (DES) at the Department of Military Affairs, using Homeland Security funding, purchased a \$100,000 software package in the fall of 2005 that can be used for maintaining an organized inventory of resources residing in the data center, and coordinating and documenting recovery plans for all state agencies. The software has been used on a limited basis, but has not been used to its full potential. DoA stated they would clarify and communicate its disaster recovery responsibilities to its staff and other stakeholders. Currently disaster recovery has been assigned to the new ITSD Services Continuity Bureau (SCB). SCB is using the DES software in a test environment. Refer to Recommendation #4 for more details.

Physical Security

Physical security involves the protection of the data center from unauthorized access, resulting in direct physical contact with data center equipment such as the hardware, cables and power cords, and physical storage media. The data center presents additional exposures and greater risks of unauthorized access because it is publicly accessible during business hours. For this reason, it is important to have a strong control structure to protect against unauthorized access.

Recommendation #2

We recommend the Department:

- A. Implement safeguards such as locked doors in Mitchell Building hallways or completed walls on the perimeter of the data center to restrict physical access to the data center.
- B. Implement procedures and assign responsibilities for ensuring background checks are complete.
- C. Follow policy and maintain required authorization documentation on file for each individual who has key card access to the data center.
- D. Conduct a periodic review of all key card access to the data center to confirm appropriateness.
- E. Monitor and review the key card activity logs and data center visitor logs for inappropriate or unauthorized access.
- F. Develop a system to ensure operator awareness of physical security breaches.

A. Implementation Status: Partially Implemented

For physical security, the department relies on walls and doors that comprise the perimeter of the data center. During the audit, we observed instances where suspended ceiling panels could be lifted up and access could be gained by climbing through the space between the suspended ceiling and the true ceiling. We also identified additional doors outside the perimeter of the data center in the hallways of the building that could be locked during nonbusiness hours to reduce the window of opportunity to enter the data center, but are left open twenty-four hours a day for convenience. DoA stated Department divisions would work together to identify and implement, where appropriate, data center physical access restrictions. Currently work is in progress to put in filler walls where feasible; plans are also in place to extend the key card secured areas as soon as the data center printing functionality and agency mailboxes are removed from the data center. ITSD represented their goal for the printing move and extending the data center secured area is July 1, 2007.

B. Implementation Status: Partially Implemented

At the time of the audit, DoA did not have any controls in place to ensure all DoA employees in positions requiring background checks had those checks completed. There was no process to ensure all employees with the defined job positions have background checks completed or procedures for regularly reviewing employees in the defined job positions to ensure the background checks are completed. DoA stated they would implement a procedure to assure required background checks are performed for individuals and positions that handle sensitive information housed in the data center. ITSD enacted background check procedures in January, 2007 that include approval and sign off by the Deputy CIO for Enterprise Operations after reviewing the background check. According to procedure, access is not allowed without the Deputy CIO's approval. I have reviewed the procedures; they are reasonable for ensuring background checks are performed and reviewed before access to data center sensitive information is allowed. However the procedures only include individuals currently beginning work in positions requiring background checks; consequently, individuals without a completed background check at the time of the audit may still not have a completed background check. Refer to Recommendation #5 for more details.

C. Implementation Status: Partially Implemented

ITSD has an internal policy to authorize data center key card access. Each person with data center access should have an authorization form on file with justifications of which doors need to be accessed, why the access is necessary, and approval signatures from the individual's supervisor as well as the CIO. The audit identified individuals with access to the data center without authorization documentation. DoA stated they would maintain card key authorization documentation as recommended. Although I did not review the documentation, data center management has represented these records have all been updated. The physical access policy has been revised, now requiring Deputy CIO for Enterprise Operations approval before access is granted; the policy was approved in January, 2007. Data center management has represented access is not granted without the Deputy CIO signature.

D. Implementation Status: Partially Implemented

Access should be periodically reviewed to ensure the approved security level is maintained. At the time of the audit, only one data center key card access review had been performed; this should be performed at regular intervals to ensure the approved security level is maintained. DoA stated they would formalize the access card review frequency and process. Currently a policy is in place requiring the Office of Cyber Protection perform monthly reviews. However, physical security responsibility was re-assigned to data center management; therefore they are to be responsible for the reviews. Data center management was not aware of this being their responsibility and believes it to be individual agency responsibility. ITSD management represented the policy would be redesigned to specifically note data center access review responsibility.

E. Implementation Status: Partially Implemented

At the time of the audit, DoA staff did not consistently monitor data center door activity and did not review overnight logs. Visitor logs are located outside the perimeter data center doors, but no controls are in place to ensure the logs are filled out or accurate. The logs reside in a publicly-accessible area, and are not reviewed. DoA stated they would review the logs as well as establish and communicate guidelines for data center visitor access. Data center management represented they collect and review visitor logs monthly and observe data center door access logs at least two or three times each day and investigate exceptions. I observed the collection of one month's visitor logs; however I did not observe review of those logs. Although it was represented the data center door access logs are reviewed at different times daily, the review does not produce documentation; therefore I was not able to ensure the reviews occur as represented. I reviewed the procedures for visitor access to the data center; they seem reasonable in addressing inappropriate or unauthorized access.

F. Implementation Status: Partially Implemented

DoA ultimately relies upon the data center being manned 24 hours a day for physical security; however we observed the only notification of someone entering the data center was a mild beep that cannot be heard over the noise made by the data center equipment. Current controls do not take into account persons accessing the data center by means other than the doors, such as the ceiling. DoA stated they would develop a system to ensure data center operators are alerted of physical security breaches. This system was to rely on installing a video monitoring system and increasing staff to allow prompt response to an intruder alert. Executive Planning Process (EPP) documents were prepared for both. The EPP for the video equipment was not approved for inclusion in the executive budget; however the EPP for extra staff was approved. Consequently no video equipment is scheduled for purchase and installation but extra staff will be added in the new fiscal year.

Environmental Security

Environmental Security consists of implementing controls to protect against environmental threats such as fire, heat, water, power loss and earthquakes. At the time of the audit, earthquake and water-related safeguards were determined to be insufficient.

Recommendation #3:

We recommend the Department strengthen safeguards to mitigate the risks associated with earthquake and water-related threats.

Recommendation Status: Partially Implemented

In evaluating earthquake controls during the audit we determined data center equipment was not stabilized or bolted to the ceiling or floor to reduce equipment movement. We also determined the state has a disaster recovery contract which includes alternate facilities in Philadelphia; this contract is further discussed in the Recovery and Incident Response section (Recommendation #4). The department said they would revise and resubmit an EPP developed during the budget planning process for Fiscal Year 06-07. The EPP was included in the executive budget and became part of Special Session HB 2; however, it was removed in the House Appropriations sub-committee due to the approval of DoA's approved new data center funding. Consequently earthquake protection will not be improved until a new data center is operating.

During the audit it was determined the Mitchell Building is constructed in a manner in which the susceptibility to water and flooding is increased due to the basement location and water pipes surrounding the facilities. By the end of the audit, DoA was beginning the installation of a new water-sensing alert system; it has now been completed.

Recovery and Incident Response

Recovery and response controls include procedures to compensate for nonexistent or failed controls which create a problem that requires recovery. The Statewide Disaster Recovery plan was not kept current; the disaster recovery contract only covered limited agency data center applications and services; and the software purchased for preparing the state's Continuity Of Government (COG)/Continuity Of Operations (COOP) planning received limited use.

Recommendation #4:

We recommend the Department:

- A. Maintain an updated statewide disaster recovery plan.
- B. Coordinate with the Governor's office to request that agencies assign a higher priority to disaster recovery.

A. and B. Recommendation Status: Partially Implemented

At the time of the audit, the Statewide Disaster Recovery (DR) plan had not been updated since 1995, and was not being used. DoA has a contract with an external vendor that does not include facilities similar to what the state currently has in operation and would require time for DoA to acquire back-up tapes, fly to the facility, install the equipment and re-load the systems and data covered under the contract. Agencies have the option to participate in this contract; however only five agencies participated at the time of the audit. The software mentioned in Recommendation #1 part E (Living Disaster Recovery Planning System – LDRPS) can be used for maintaining an inventory of data center resources and documenting and coordinating all state agency DR planning. DoA has formed a new bureau, the Services Continuity Bureau (SCB), to focus on the state's DR/COG/COOP planning. The Bureau is developing a new framework for Montana's continuity planning based on the federal National Incident Management System (NIMS), the DR Institute's industry continuity planning best practices and other states' DR implementations using LDRPS. This framework is to tie the state's enterprise and individual agency business goals and requirements together with the supporting information technology by using LDRPS for DR plan development. Although the framework is not currently defined or documented in LDRPS, testing has begun and it is expected to be defined, documented and implemented by July 1, 2007. The framework will include mandatory agency DR staff training and require each agency to be fully responsible for their DR plan. The plans will be tested, revised as needed, and be reviewed yearly. SCB management is in weekly contact with the Governor's Office; both SCB management and Governor's Office have stated continuity of operations has become an issue of priority.

Data Center Security Measures Not A Priority

The audit discovered data center security measures were not being prioritized because of a focus on obtaining a new data center; DoA was focusing more on providing convenient services to agencies rather than prioritizing security; and DoA relied on the 'Security by Obscurity' approach. This approach relies on the knowledge security weaknesses exist but they are not focused on as the weaknesses have not yet been discovered.

Recommendation #5

We recommend the Department clearly define and designate responsibility for coordination of all aspects of data center security.

Implementation Status: Partially Implemented

Currently, complete documentation does not exist defining and designating security responsibility for the data center. DoA is relying on job positions and duties to determine security responsibility. For example, SCB is responsible for continuity planning and data center management is responsible for data center physical security. However, this still leads to confusion when consulting policy. For example, the background check policy (considered part of physical security) refers responsibility to Network Security, not data center management; consequently confusion exists as to who is responsible for completing background checks not complete at the time of our audit. ITSD management has stated these policies and designations will be revised in June.