Serious State Tech Problems Need Public Scrutiny

Posted on Apr 11, Posted by Kathleen Vinehout, State Senator 31st District Category Wisconsin

Is the State IT system at risk? A recent audit had several recurring findings related to IT security, which showed agencies had not implemented past recommendations to fix them.

MADISON - Is the state of Wisconsin at risk for a cyber-attack? A new audit from the Legislative Audit Bureau (LAB) shed light on what may be vulnerabilities in the state's Information Technology (IT) system that could affect every business, taxpayer, student or recipient of state services.

In some cases, problems are so serious that LAB auditors could not reveal details in fear of creating additional vulnerabilities for hackers to exploit.

The audit described problems related to a lack of protection in computer security, a lack of adequate security policies, procedures and standards, which increased the risk of fraud.

Disturbingly, many of these weaknesses are recurring. In several cases, past audits found similar problems.

For example, to protect student data, and keep accurate financial records, auditors recommended remedial actions at the University of Wisconsin System. University officials took some action, but auditors reported they had not taken significant steps to cover critical areas, which increases the risk of unauthorized or erroneous changes in payroll, accounting and student information.

Similarly, auditors reported on weaknesses in security at the Department of Administration (DOA). Officials did not do a comprehensive risk assessment to identify security concerns and vulnerabilities since 2012. Because regular “penetration tests” were not completed, the state could not find and evaluate the risk of vulnerabilities and did not know how safe or unsafe all servers and systems were in the state’s network.

When reporting on what caused some of these problems, auditors wrote that “agency management is resistant to the development of IT policies and standards.” It is unclear why agency management is resistant.

Similar to the UW, auditors found some recurring IT security problems at DOA. In one finding, auditors wrote DOA did not take any of the additional steps outlined in its own corrective action plan.

Another finding related to a lack of control over IT security could result in unauthorized changes related to vendor payments or payroll. These problems were too serious to publically detail but might result in undetected financial misstatements, fraud or theft.

As a side note, auditors also found evidence of mistakes in the state's financial statements, which were not related to IT security. The audit described problems in cash management. In auditing the state's financial records, auditors traced errors back to mistakes in monthly reports, in bank reconciliations and in payroll.

Because of these errors, the state showed a net amount of $21 million more than the actual cash. When trying to understand the cause of errors, auditors wrote staff "did not always understand the effect of the errors on financial reporting and did not take steps to communicate them to the appropriate agencies."

Audit findings showed many mistakes in the financial report of the state's capital transportation assets. Problems related to how DOT used different types of computer records. Multiple factors contributed to the errors, including poor planning and inadequate written documentation.

Evidence of other errors was found in the state infrastructure reports. For example, the Department of Transportation erroneously classified $27.2 million as bridges that should have been classified as roads.

Five years ago, Wisconsin embarked on a large IT purchase and system conversion. There was no dispute the new system was needed; however, the costs were massive, estimated at $139 million.

I serve on the Joint Committee on Information Policy and Technology. In one of the very few public hearings held on the IT investment, DOA officials repeatedly told lawmakers the project was "on time and within its budget".

While questioning DOA officials, we also learned the system involved thousands of staff hours not recorded nor budgeted. Hundreds of employees were moved from various agencies, in which they worked to DOA, which increased that agency's staff by nearly fifty percent. We learned about delays in the project implementation and delayed payments to vendors, which resulted in late fees that cost the state five times more than late fees charged in the previous

year.

For years, my Democratic colleagues and I called on GOP leaders to exercise their legislative oversight of the state's IT system. Both the Audit committee and the Information Policy committee must get to the bottom of IT security problems and insist, under threat of budget reductions, that things are fixed.

The audits are a "wake-up" call for state IT officials. The best way to protect is to prevent risk.

Tags: Untagged