Approved 3/15/2012
(Date)

MINUTES OF THE HOUSE GOVERNMENT EFFICIENCY COMMITTEE

The meeting was called to order by Chairperson Mike Burgess at 3:30 p.m. on Thursday, February 29, 2012 in Room 546-S of the Capitol.

All members were present except:
Rep. Grange - Excused
Rep. Loganbill - Excused
Rep. Meigs - Excused
Rep. Roth - Excused
Rep. Ruiz - Excused

All Committee staff was present except Julian Efird, Legislative Research, and Jim Wilson, Revisor of Statues.

Conferees appearing before the Committee:
Scott Frank, Legislative Post Auditor

Others in attendance:
See attached list.

Scott Frank gave a presentation (Attachment 1) on IT Security Auditing. He introduced the persons in the audience with him today. They were: Justin Stowe, Deputy Post Auditor; Dan Bryan, Senior IT Auditor; Nathan Ensz, Senior IT Auditor; and Stan Wiechert, Principal IT Auditor.

Mr. Frank explained that the first page of the handout was a diagram that state agencies should be following for the security management process. He added this is a proactive approach to IT security, but most of the time, when dealing with IT security, it is reactive. Every two or three years, each state agency, whether the Department of Revenue lottery or the small licensing boards, needs to discuss risks, develop policies, promote awareness of those policies, and then monitor and evaluate policy compliance.

The next part of the handout was a summary of select IT audit findings. The first finding was that of the five agencies audited, none provided security awareness training to new hires and current employees. There should be two steps to training: one to all new employees within 90 days and the second to retrain employees annually, which should include passwords, physical security, social engineering, and viruses.

As part of an audit, a consultant was hired to come into an agency office for a test of physical security. The consultant was able to enter locked offices and roam around, to remove confidential documents and photograph them, and to convince staff to provide passwords over the phone.

Most agencies now require complex passwords which consist of uppercase, lowercase, numbers, and special characters. Because employees use passwords with predictable patterns, password cracking software was able to crack 23% to 50% of the passwords at the five agencies within five minutes.

Three of the five agencies audited had significant vulnerabilities because of inadequate workstation patching processes primarily because of non-Microsoft software. These agencies also did not perform a periodic scan of workstations for vulnerabilities.

Audit staff was also able to recover old files from surplus computers during a 2008 audit. Even though a file is deleted, the file is still on the computer. Some computers contained confidential information. Hard drives should be taken out of old computers and printers. Free software is available on the internet to erase all files to Department of Defense standards.

The state's Information Technology Executive Council (ITEC) developed minimum security standards for state agencies and communicated those to less than half of the agencies and did not notify agencies of amended policies. In small agencies, they never heard of the standards.

A copy of an audit report on one state agency's information systems was part of the handout. Mr. Frank called attention to Page 13, question 2, regarding disaster recovery planning. This is really important as to what systems are available to get online if a disaster would occur. The department's plan didn't address the issues that a business continuity plan should address, that is, disaster scenarios with appropriate reaction and responsibilities of specific staff so that people know what to do.

Several agencies have been selected for audits in 2012. A scope statement asks seven important information technology security audit questions which state agencies must answer.

Questions from the Committee and answers by Mr. Frank included:

--Concerning privacy of records, if there is a breach, it is reported as specified by protocols (Chief Security Officer, to the JCIT Committee in executive session, FBI, KBI, etc.). The agency continues follow-up for several years.
--Access to files can be read only and that is controlled.
--As a person moves from state office to state office, a list of the systems they access is noted and discussed with the supervisor to determine if access is needed to all systems listed.
--An audit finding report is issued to all state agencies to report on problems without identifying a specific agency. It is used as an education tool for other agencies.
--There is always a need to educate employees on physical security (passwords, people walking through office, patch management, etc.).
--Some agencies allow administrative rights to software; others restrict it. The specific job may require access by specific employees.
--At the top of the list for security is medical record data involving state employee health care, Medicaid, etc.
--Post Audit staff is aware of hard drives on printers and copy machines that could have information. As machines are upgraded, the hard drives are pulled and information destroyed. Mr. Frank was unsure how each state agency handles this.

Chair Burgess thanked Mr. Frank for his presentation and the work he and his staff do for the state.

There being no other business, the meeting was adjourned at 4:25 p.m.