SUBJECT: Requiring recognition of risks in agency information security plans

COMMITTEE: State Affairs — favorable, without amendment

VOTE: 11 ayes — Cook, Giddings, Craddick, Farney, Geren, Harless, Huberty, Kuempel, Minjarez, Oliveira, Sylvester Turner

0 nays

2 absent — Farrar, Smithee

SENATE VOTE: On final passage, April 30 — 31-0 on local and uncontested

WITNESSES: None

BACKGROUND: Government Code, sec. 2054.133 requires each state agency to develop and periodically update an information security plan for protecting the agency's information from unauthorized access, disclosure, destruction, and other security threats.

A successful cybersecurity attack could pose serious threats to state infrastructure and the personal information of Texans. Observers have noted that the lack of direct communication between organizations' cybersecurity officers and upper management could increase the risks posed by such an attack. SB 1597 by Zaffirini, enacted by 83rd Legislature, requires state agencies to submit an information security plan biennially, but does not require that state agency executives be informed of cybersecurity and other risks revealed during the plan development process.

DIGEST: SB 35 would require that each agency's information security plan include a written acknowledgement that the official head of the agency, the chief financial officer, and each executive manager of the agency be made aware of the risks revealed during the preparation of the agency's information security plan.

The bill would take effect September 1, 2015.