Texas exposed; Cybersecurity bill will protect public's data

Texas does a lot of things right. Low taxes and regulatory climate, friendly business environment for job seekers and entrepreneurs, strong infrastructure, and highly sought after public universities and research institutions. Yet, there is an issue that lurks in the shadows which is not a priority, or even on the radar for most of our state leaders in Austin. That's the issue of cybersecurity.

On March 31, 2011 it was revealed by the Office of the Comptroller that the personal data of approximately 3.5 million Texans were publicly accessible via its website for up to a year. The breach cost taxpayers approximately $2 million and left the agencies affected flat footed. The data files were not encrypted as required by Texas administrative rules, and other internal procedures were not followed, leading to the breach.

Now, six years later, are we secure? The answer is no.

Enter HB 8, the Texas Cybersecurity Act.

Authored by Rep. Giovanni Capriglione, R-Southlake, the bill will go farther to protect citizen's data by instruct the Department of Information Resources to lead in the creation of standard security protocols for all agencies; place formal responsibilities on executives at all state agencies to construct, carryout, and report on their security plan each year; and allow for oversight through annual third party audits, through the creation of a cybersecurity committee in the legislature, and through the Sunset Commission's review process. Not to mention the destruction of personally identifiable information not required by law to retain.

Many of the ideas outlined in the Texas Cybersecurity Act are no cost or low cost policies that stem from cybersecurity protocols found in the IT departments at many of our member companies. These protocols securing the private sector will better secure Texan's private data by integrating national standards used to identify threats and protect our systems from even the most cutting edge malware. Arguably one of the most important protocols however, is the establishment of mandatory guidelines for cybersecurity certification by all information resource employees for each agency. Most of our most sensitive data is stored at the state level and by equipping our public servants with the always changing know-how to minimize data exposure and identify threats; we can nip a potentially serious breach, in the bud.

With a reliance on digitally connected infrastructure and markets, the world is experiencing an unprecedented threat to individual privacy and personal information. Cyber theft and related crime affects every part of our economy, our government, and our daily lives. The State of Texas must lead the way in developing a holistic cybersecurity strategy for our state agencies that will complement the foundation measures currently in place. Texas must be prepared and must remain vigilant.

Justin Yancy is the president of the Texas Business Leadership Council. The TBLC is a network of Texas based CEOs and senior business executives who advance a long-term vision of a prosperous Texas in a globally competitive business environment. You can follow Justin @JustinYancy and the TBLC @TX_BLC.