Texas Department of Information Resources
Written Testimony: Senate Committee on Open Government

TEXAS CYBER RISKS AND OPERATIONS

Privacy is Why
Texas is connected to the Internet so it is exposed to daily cyber-attacks by criminals and nation states. It is increasingly coming from a broader range of individuals and entities who understand cyber vulnerabilities and how to exploit them.

Texas depends on a complex system of integrated, intertwined infrastructure. This critical infrastructure includes our energy grids and power plants, dams, water supplies, control systems, gas and oil production, transportation, distribution systems, airports, harbors, railways and fuel supplies, public health and police systems, technology and telecommunication systems, and military installations.

Texas government uses electronic personal and financial information to deliver many services through the internet to its almost 25 million citizens – much of that information is governed by federal and state requirements for privacy protection.

Security is How
The Texas security governance process includes state agencies and institutions of higher education collaborating with each other and with The Department of Information Resources (DIR) to protect state information technology assets.

State agencies and institutions of higher education operate security programs that help them identify, resource, and execute security initiatives to serve their regulatory requirements and business needs for protecting the financial information, personal data, systems, and networks they rely on to conduct critical functions on behalf of our citizens.

STATEWIDE CYBERSECURITY COLLABORATION

To proactively address the cyber security challenges faced by state agencies, DIR has established a multi prong approach aimed at enhancing partnerships with state agencies and creating partnerships with the private sector to strengthen the overall security posture of the state.

Network Security Operations Center (NSOC)
The DIR NSOC provides services to Texas state agencies, local governments, public education entities, and special districts, such as hospital and water districts. The NSOC prevents an average of 75 million incidents monthly and upwards of a 110 million in any given month. This program recently received the Center for Digital Government 2012 Cybersecurity Leadership And Innovation Award in State Government.

Texas Cybersecurity Council
In 2011, Senate Bill 988 (Senator Van de Putte; Representative Larson) authorized formation of the Texas Cybersecurity, Education, and Economic Development Council. This council is a public private partnership to improve the infrastructure of the state's cybersecurity operations, examine strategies to accelerate the growth of cybersecurity as an industry in Texas, and encourage the industry to call Texas "home."

The goal of the council is to form a statewide public survey for baselining the state of cyber infrastructure and education in Texas. The council will assess federal and state government and industry best practices or new initiatives in order to identify strategies for enhancing the cybersecurity industry within Texas. A report from the Council will be published by December 1, which will review the results and identify ways to mature security, scale best practices, and seek approaches to cybersecurity education (kindergarten to senior citizens).

Statewide Information Security Advisory Committee (SISAC)
DIR chartered SISAC to provide guidance to protect government information assets and technology. SISAC considers top statewide security risks, advises DIR on cyber security program offerings to unite DIR and state agency efforts to protect Texas government information assets and technology. SISAC has chartered 5 subcommittees to assist in prioritizing information security initiatives, projects, and policies.

Current membership of SISAC includes: Texas Department of Public Safety, General Land Office, Comptroller of Public Accounts, Texas Workforce Commission, Texas Education Agency, University of Texas Systems, Health and Human Services Commission, Office of the Secretary of State, Office of the Governor, Office of the Attorney General, and Board of Nursing. Because every agency does not have a designated Information Security Officer, membership includes personnel from various divisions including information technology and legal.

Third Party Cyber Security Assessments
DIR partners with a third party security entity in order to provide cyber security assessments of state agencies. DIR provides participating state agencies with access to a full breadth of security analysts and research, allowing for direct one-on-one inquiries with experts, as well as access to security research articles, tools, and intellectual property. The program also conducts a series of monthly webinars with private sector experts to address statewide security needs and topics of interest.

These assessments have identified numerous observations and trends that provide early insights into possible risks and opportunities for the state. The SISAC has reviewed and provided guidance to DIR on trending results. The key issues that the assessments focus on include:

- Maintaining sufficient levels of staffing focused on security and risk management
- Ensuring that security is a priority during all steps of software development

- Emphasizing, updating and enhancing security awareness programs
- Following a standardized approach for identity management and access control
- Consistently and comprehensively analyzing network and system monitoring data
- Establishing consistent use of internal network segmentation options
- Classifying data in order to optimize security protection techniques
- Implementing encryption technology and anti-malware
- Maintaining developed continuity plans for recovery and continuous operations

To date, DIR has completed 10 agency assessments, is in process of assessing 5 agencies, and has 15 additional agencies planned for completion by the end of FY 2014. With the results of these assessments, DIR will publish a State of the State Report that presents trends identified and agency survey responses and describes the current state of cyber security in Texas.

Exceptional Items

DIR's Legislative Appropriations Request includes exceptional items related to cyber security. This funding would allow DIR to continue and expand the current cyber security program for the state. The exceptional items request addresses many opportunities for improvement identified in State of the State security trending data and would provide for upgrading state security policies, retaining risk visibility through continued third party assessments, enhancing IT security staff training and workforce awareness offerings, enhancing security program automation for state agencies, and increasing security program support through additional professional security staffing.

CYBER SECURITY NATIONWIDE

Federal Level

National Association of State Chief Information Officers (NASCIO) created security program taxonomy to understand what states should be offering for their governmental entities in order to better prepare themselves for cyber security threats. This program is also assessing each state to analyze their current security practices. NASCIO created a security and privacy committee of State CIOs to facilitate communication and created best practices amongst states.

The federal government administers the Multi-States Information Sharing and Analysis Center. This center provides early warning to state security programs and leverages experienced state Chief Information Security Officers (CISO) to mentor others.

The US Department of Homeland Security funds awareness and training initiatives for state CISOs. The Department also facilitates collaboration with state CISOs, emergency management officials, and fusion centers to create cyber security initiatives.

State Level

Other states continue to consider new privacy and security legislation to mandate protections for the information of its citizens. States are creating more awareness for their citizens and are looking at the risks to their public utility infrastructures (power, water, energy) and response plans.

Texas, like most states, faces real resource constraints that place a premium on efficiency of government operations. These constraints drive IT consolidation, cloud computing, and mobile technology solutions, and bring new security challenges to Texas. On behalf of our 25 million citizens, Texas must continue to build even more robust statewide information protection policy and governance, operations, and service capabilities that unite state agencies and institutions of higher education as they collectively manage privacy risks to Texas information and protect Texas information assets and technology.