Protecting Citizen Data Through Technology Security

The Florida Technology Council, by Cyndy Loomis

The Challenge - Any Floridian who watches the media is aware that cybersecurity is a national issue as breaches occur in companies such as Equifax, Target, and most recently Marriott. Public sector data systems are not immune from these cyber attacks. Government technology systems contain information on citizens and the services they receive, ranging from public health information, to academic history, criminal history, government employee records, and social services. To say that Florida must be vigilant against cybersecurity threats is easy, but protecting Florida's technology assets involves thousands of information systems, Internet of Thing (IoT) devices, and connected machines developed in a range of new to aging technologies. Further complexities exist since information technology (IT) systems not only reside in state agencies, but also within local county and city governments, that often have limited resources. In addition, government entities have to compete for cybersecurity talent in a market where there is a worldwide shortage of two million security professionals, and the cost of qualified labor continues to escalate because the demand exceeds supply.

Current Efforts - Within the State of Florida, there are three groups that have a role in cybersecurity: the Agency for State Technology (AST), the Florida Department of Law Enforcement (FDLE), and the Florida Center for Cybersecurity (Cyber Florida). These efforts reflect Florida's responsible commitment to protect citizen's sensitive data.

The AST, provides strategic direction to the state agencies on information security initiatives and is mandated by 282.318 F.S. to develop and publish an information technology security framework. The AST has established tools and processes to guide the agencies' IT risk assessment efforts, while the Auditor General audits the state agencies to ensure compliance. The AST also provides cyber training for agency personnel. Through a University of West Florida partnership, cybersecurity training is available for agency technical staff to increase their expertise; a separate vendor contract makes security awareness training available for end-users throughout the agency. Lastly, the AST, the Florida Department of Emergency Management, and the Florida Department of Law Enforcement have developed a cyber disruption plan to respond to large-scaled cyber-attacks as a supplement to Florida's comprehensive emergency operations procedures.

The FDLE Fusion Center is a collaborative effort of state, local, tribal territorial, and federal agencies working in partnership to share resources, expertise, and/or information to better identify, detect, prevent, and respond to threats, crimes and terrorist activity. The Florida Fusion Center (FFC) headquartered in Tallahassee, Florida, began operations in 2007 and was designated as the head of the Network of Florida Fusion Centers in 2008 by the Governor. The Fusion Center works closely with the FBI in these efforts. Cyber Florida, housed within the University of South Florida, conducts activities throughout the State of Florida to grow the state's cybersecurity industry and to address related workforce needs through education and outreach. Florida also has pockets of excellent and innovative technology training programs that address the cybersecurity workforce needs. Among them are Andrew Jackson High School, Tallahassee Community College, and the University of West Florida which have all created premier centers producing cybersecurity talent.

Opportunities for Improvement - Even though the AST provides cybersecurity guidance, the responsibility for data security still ultimately resides within each individual state agency or local government entity. The current approach results in disparities based on an agency's ability to obtain legislative funding for their

individual cybersecurity program. Nobody at the state-level oversees the legislative appropriation process for cybersecurity in order to direct the most funding toward protecting the state's most sensitive data. There is also no single entity coordinating how agencies are deploying security measures for new statewide projects such as the Medicaid Enterprise System Refresh (Agency for Healthcare Administration) or the PALM Financial Management System (Department of Financial Services).

Options for Florida – The State of Florida's cybersecurity efforts must continue to evolve and mature. In a April 2018 report, *The Cyber Hygiene Index: Measuring the Riskiest States*, the State of Florida was ranked last among the states' cyber programs according to the Ponemon Institute. Nationally, trends are emerging to strengthen cybersecurity programs through the establishment of a single organization at the highest level of government possible to coordinate cybersecurity standards, to audit compliance, and to review/direct funding to the greatest area of need. For example, the United States Cyber Command is tasked with centralized guidance for the Department of Defense's cyberspace capabilities through its information assurance program. At the federal level, the President established the Cyber and Infrastructure Security Agency on November 16, 2018 with cross-organizational responsibilities and authorities.

Among the states, cybersecurity programs are changing. The California Department of Technology is charged with setting security standards, while also ensuring compliance audits are conducted. In New York, the Chief Information Security Officer has responsibilities ranging from statewide policy coordination, to incident responses, and vulnerability detection. In New Jersey, the state views cybersecurity as an executive-level risk management responsibility and recently moved security from its central technology organization into the New Jersey Office of Homeland Security and Preparedness. In Virginia, centralized security is contained within the enterprise technology organization and includes partnerships with private industry and educational institutions to increase education and awareness.

Based on these other models, the State of Florida should consider adopting a cybersecurity model in which a single central entity has greater accountability for Florida's cyber protection. This central authority could be housed in an existing state agency or established as a quasi-public entity that is able to provide the compensation needed to retain high-caliber cybersecurity professionals.

Next Step – Floridians deserve a holistic approach to fund and protect our valuable data. Florida has several options to consider based on successful models used elsewhere. The Florida Legislature should establish a statewide task force that examines all aspects of our state's cybersecurity requirements in order to evolve Florida's capabilities. This task force approach could emulate the State of Indiana which created an Executive Council on Cybersecurity in July 2017 to examine all dimensions of the state's needs, from workforce development to asset protection as set forth in its roadmap for systemic advancement.

About FTC - Technology is the foundation of the new worldwide economy and is a critical element for extending Florida's growth beyond tourism and agriculture. Every Florida business, citizen, and the 27,000+ registered technology companies rely on technology for business innovation, growth, and prosperity. Other state economies are growing faster than Florida by becoming knowledge-based, globalized, entrepreneurial, IT-driven, and innovation-focused. The Florida Technology Council (FTC), a 501(c) 6 educational non-profit association, is playing a pivotal role in defining Florida's technology future by highlighting four areas where technology advancements are critical: identifying effective economic policy tied to technology, creating Florida's knowledge-based economy, securing and protecting citizen data, and developing a technology skilled workforce.