2019 Florida CYBERSECURITY FORUM

AIF FOUNDATION

Addressing the education and development needs of Florida's business community.

Chairman of Foundation

Jose Gonzalez
Director, Government
& Industry Relations
Walt Disney Parks
& Resorts

A Message from the Chair

The cyber threats landscape is constantly evolving and yesterday's security solutions may not be sufficient for tomorrow's challenges. What are the most significant cyber threats and from where will they originate? How are companies and state agencies defending against attacks and intrusions? Where are the weak points in systems and training? What are steps which can be taken to better protect our data and critical infrastructure?

On November 20, 2019, the FAIF hosted the first annual Florida Cybersecurity Forum which convened leading cybersecurity experts from around the country, business executives and senior elected officials, and drawing more than 150 representatives from industry, state and local governments, academia, and the media.

The experts and business leaders on Threats & Resiliency panel at the 2019 Florida Cybersecurity Forum provided an in-depth discussion of the significant cyber-threats to companies and our state's critical infrastructure.

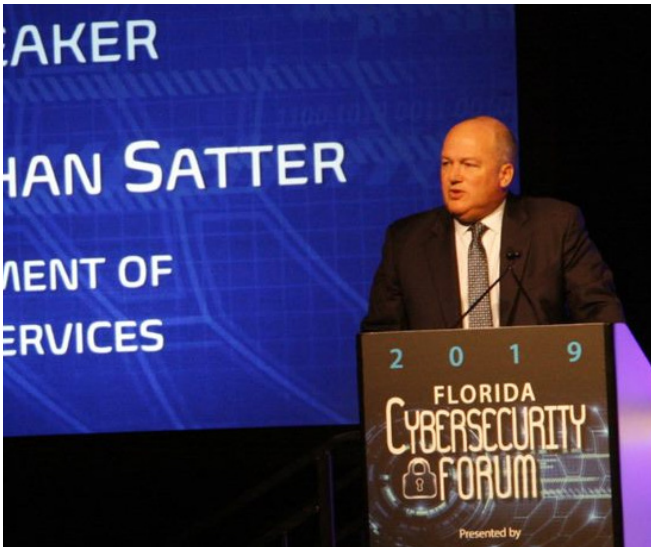
2019 FLORIDA CYBERSECURITY FORUM

Florida Chief Financial Officer Jimmy Patronis (pictured above) shared the latest efforts within the Department of Financial Services to better protect Floridians from cyber-related fraud and secure Florida's critical banking infrastructure. Patronis highlighted programs such as Fraud Free Florida, a new initiative bringing together statewide law enforcement officials, local state attorneys, private sector stakeholders, and dedicated fraud investigative teams to protect against public assistance fraud, identity theft, and cybersecurity issues. He also provided an update on the recently launched Florida Blockchain Task Force, which will examine how state, county and municipal governments can benefit from a transition to a blockchain-based system for record keeping, data security, financial transactions, and service delivery, as well as identify ways to improve government interaction with businesses and the public.

Florida Department of Management Service Secretary Jonathan Satter (pictured right) provided attendees with the status of the recently reorganized Division of State Technology and outlined several initiatives under his leadership, including a continued shift to a cloud-first strategy for managing the state's sensitive data (human resources, health benefits, pension and prison systems), data analytics and interoperability and using data for evidenced-based policy, as well as the state's newly-created Florida Cybersecurity Task Force. The task force's charge is to analyze the current state of, and potential for, improvement in the security program of state government and individual agencies and to prioritize the risks posed by identified threats.

The **Threats & Resiliency Panel** featured senior cybersecurity and cyberwarfare experts from the healthcare, aerospace, and defense sectors, as well as from the U.S. Navy Cyber Forces (CYBERFOR) and Federal Bureau of Investigation. Attendees were given a snapshot of the evolving global cyber threat landscape and how businesses and governments are developing more advanced offensive and defensive capabilities against cyberattacks. The panel covered a range of priorities and concerns including the importance of basic cyber hygiene, the need for better threat intelligence and information sharing, disinformation campaigns, cyber espionage, and partnerships like InfraGard, a collaboration between the FBI and members of the private sector. The panel also touched upon challenges including supply-chain security in an increasingly connected global economy, and difficulties with social engineering.

The **Evaluating Liabilities & Insurance Panel** brought together legal and regulatory experts in cyber risk modeling, management and mitigation. Attendees were provided with information on how to accurately evaluate cyber liability exposure and solutions for data breach and service interruption, including options for insurance coverage. The panel examined the history and evolution of the cyber liability insurance market, as well as future trends and projections for growth. Speakers touched on difficulties in estimating the value of attacks and challenges with lack of historical data and the changing global regulatory environment, including the California Consumer Privacy Act, the European Union's General Data Protection Regulation, and the reauthorization of the U.S. Terrorism Risk Insurance Act.



Florida Secretary of State Laurel M. Lee (pictured above) shared with attendees an update on recent actions taken to enhance cybersecurity for Florida's election systems to better protect sensitive voter information data. Lee discussed the new **Joint Election Security Initiative** (an evaluation of election equipment and systems security throughout the state), along with a framework for all 67 counties to carefully control access to sensitive and classified information within their offices while also allowing them to share sensitive information with the Florida Department of State regarding security policies and any attempted breaches that may happen in the future. Attendees learned about the **Cyber Navigator Program,** a resource of dedicated cybersecurity support staff to county Supervisors of Elections offices, as well as the Electronic Registration Information Center, an information-sharing initiative between 30 states that will allow Florida to cross-check voter registration data with that of other member states. Lee also addressed challenges such as public confidence, misinformation campaigns and unofficial results reporting, attacks on physical sites, and training at polling stations.

The **Cities & Small Business Panel** included businesses with first-hand experience dealing with cyber-attacks, representatives from municipal governments, technology solutions providers, and small business experts with the National Institute of Standards and Technology Cybersecurity Framework. Attendees learned about leading threats such as phishing and ransomware, cost-effective resources and information availability, and supply-chain challenges for small businesses including U.S. Department of Defense Federal Acquisition Regulation Supplement compliance, as well as the forthcoming Cybersecurity Maturity Model Certification framework. **Representative Jamie Grant (R-Tampa)** (pictured below) broadly shared with attendees his insights on current public policy around technology issues, including cybersecurity and difficulties with innovation and the interoperability of data across various branches and levels of state and local governments. Grant cited support amongst the current legislature and administration for improved coordination and efforts to combat and defend against cyber threats; however, he cautioned against a pervasive belief amongst some officials that enterprise technology solutions are static or lacking a clear return on investment.

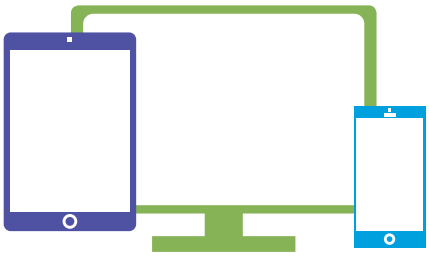
The **Education & Workforce Training Panel** featured workforce development experts from within industry and academia, including the Center for Cybersecurity at the University of West Florida and Cyber Florida at the University of South Florida. Attendees came away with examples of training programs in Florida and how the public and private sectors are collaborating to better seed the cyber talent pipeline. The panel delved into issues including the need for increased funding and investment in cyber education and training, prioritization of cyber within C-suites and board rooms, incorporating cyber across other disciplines, the importance of continuing education programs, and up-skilling existing workers for new cyber jobs.

Expert speakers shared the latest efforts to defend Floridians against cyber attacks.

Banking and Finance

Fraud Free Florida is a new initiative to protect Floridians against public assistance fraud, identity theft, and cybersecurity issues.

Florida Blockchain Task Force will advise how governments can benefit from a transition to a blockchain-based system for record keeping, data security, financial transactions, and service delivery.



Sensitive Data

Division of State Technology outlined several initiatives including a continued shift to a cloud-first strategy for managing the State's sensitive data, data analytics and interoperability.

Cybersecurity Task Force is charged with analyzing the current state of, and potential for, improvement in the security program of state government and individual agencies and prioritizing the risks posed by identified threats.

Florida Elections

Joint Election Security Initiative (an evaluation of election equipment and systems security throughout the state) coordinates with a framework of all 67 counties to carefully control access to sensitive and classified information and sharing information with the Florida Department of State.

Cyber Navigator Program is a resource of dedicated cybersecurity support staff to county Supervisors of Elections offices.

International

National Institute of Standards and Technology Cybersecurity Framework is helping organizations better understand and improve their management of cybersecurity risk.

InfraGard is a partnership between the **FBI** and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information contributing to industry-specific insight and advancing national security.

The Foundation of Associated Industries of Florida (FAIF) was formed to address the education and development needs of Florida's business community. FAIF fosters programs that identify business needs today and create solutions that will last into the future.

FAIF focuses on current issues that are important to the success of Florida employers, and works to educate the public at large about these issues to make Florida a better place for its businesses and citizens to call home.

FAIF.org