Florida – Becoming the Nation's "Cyber State".

According to Steve Kroft of CBS News' "60 Minutes" and Wilfredo Ferrer, the U.S. Attorney for South Florida, Florida owns some dubious titles in the field of cyber crime.

- Florida is #1 nationally for ID theft three years in a row.
- ID theft in Florida has tripled in the last three years.
- Miami is the #1 metro area in the country for cyber crime.
- Florida is the "Silicon Valley of Cyber Scam".

"Scam" and "fraud" have long been words connected with Florida's reputation, but now the word "cyber" is finding itself in the same company. "60 Minutes" brings vital information to the forefront with this episode including issues that are much bigger than Florida's piece of the problem.

"For decades now, south Florida has been the Silicon Valley for scam artists, drawn here by the weather, the beaches and the opportunity to make lots of money without actually doing much work. There's Medicare fraud, mortgage fraud, securities fraud, and now what the Justice Department calls stolen identity tax refund fraud a tax preparation scheme epitomized by an over abundance of questionable looking establishments that have sprung up here over the past few years. But this scam is so easy you don't even need an office."

60 Minutes - The Tax Refund Scam CBS News, June 28th 2015

For Florida, however, its 2013 Legislature and Gov. Rick Scott are wasting no time making the most of a severe crisis. Now, $5 million later, the Florida Center for Cyber Security, or FC2, is in its second year and making headway toward its long-term mission as memorialized by the 2014 Legislature in HB 5101:1004.444, Florida Statutes: Florida Center for Cybersecurity:

a) Position Florida as the national leader in cybersecurity and its related workforce through education, research, and community engagement.

b) Assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce.

c) Act as a cooperative facilitator of state business and higher education communities to share cybersecurity knowledge, resources and training.

d) Seek out partnerships with major military installations to assist, when possible, in homeland security defense initiatives.

e) Attract cyber security companies to the state with an emphasis on defense, finance, health care, transportation, and utility sectors.

"In short, a presence in the cybersecurity industry will quickly bring Florida's economy new revenue, new jobs and an unparalleled cybersecurity knowledge base. It will drive the State University System further toward national prominence as a coordinated unit, preparing graduates for the practical, high-paying jobs of today and tomorrow."
Making Florida the Cyber State - *Florida Board of Governor's Cyber Security Report, December 2013.*

Points a. through e. above read "jobs" and that's great by all accounts. But, there is much more at stake, and a case study in a matter for our age is unfolding. Florida is the lead duck living today what others will live with tomorrow. It is an organic, living laboratory for the new face of cyber risk, which is fast becoming a broad-based, horizontal arena (individuals, their devices, on non-IT-managed networks), as opposed to its tradition of being vertical and enterprise in nature (server-centric, enterprise owned devices on IT managed networks). Simply put, cyber security is going from an IT-defined environment to a user-defined environment. Vast adjustments must be made in the matter of resolution and Florida is at the frontier of these new, complicated challenges that will have to be approached with innovation far past the technology itself to get the job done.

Fortunately, to match the State's leadership position in the problem of cyber-crime, the Florida Center for Cyber Security represents a formidable step in the right direction for the State to assume a national leadership position in the problem's resolution.

Florida Center for Cybersecurity

The Florida Center for Cybersecurity is established within the University of South Florida and led by Director Sri Sridharan.

IS FLORIDA ON ITS WAY TO BEING THE NATION'S "CYBER STATE"?

Florida has prominently established itself nationally as being ground zero for cyber crime committed against mainstream individuals living their daily lives. The vast majority of victims here are not spies, global leaders, corporate titans, or others that may be specifically targeted by hackers, hacktivists, or cyber criminals. In Florida's case, the problem has gone mainstream and is reaching massive proportions that pose a significant and escalating threat to the State's economy and social fabric alike. As Apple's Tim Cook said about information security in February earlier this year "We must get this right.", so too must Florida get this right.

Nothing to hide, everything to lose. Florida victims of tax-fraud lining up at an IRS office to begin the long process of receiving their legitimate federal tax refunds.

Florida has long been notable for its attraction to much of society's greater, fringe elements. Scammers, fraudsters, and the most notoriously innovative of low-level criminals have

come for its wealthy population, international connections, and concentrations of vulnerable targets including senior citizens, nicely wrapped in a lifestyle better than from where they come. Today, personal information is viewed as one of the most valuable currencies in crime, and its attraction to criminals is reinforced by the benefits of cyber vs. traditional crimes including relative safety and ease of perpetration, significant upside especially when compared to potential consequences, and nirvana for dirty money; anonymity, portability, and liquidity for the loot. For cyber criminals, Florida is their place in the sun.

Gov. Scott and Florida's leadership gets it, and FC2 Director Sri Sridharan gets it, that true to nature, the problem they face is matched only by the opportunity they hold. In the Information Age, cyber crime at the individual level, and as it applies to the everyday, mainstream life of citizens, consumers, voters, and taxpayers, is where the action is and will be for many years to come.

Florida is in a distinct position from which to play a long-term, vitally important role in the battle against cyber-crime not only for itself but the nation and global community as a whole. We have some thoughts about how to approach the challenge and embrace the opportunity in new ways to leverage certain mega-forces that are irretrievably at hand and can fuel progress and success for many years to come. Some elements of our ideas are in place, some need to be built, but most importantly it is a matter of shared vision, coordination, and alignment of resources to tap the potential for Florida. By facing the future of both the problem's resolutions and solutions, Florida can mine significant opportunity from both ends.

Our list of ideas:

- **Position Cyber Security as a Social Science** - First, position much of the challenge in cyber risk mitigation as a social science as opposed to a purely technological problem to solve. Yes, there are problems and opportunities in the area of IT security technology and Florida should seek a meaningful role in its development and transfer to the private sector, but in the end, the technology will take care of itself. This can be banked on as a result of the difficult to fully appreciate potency inherent in the mix of free-markets and Moore's Law. The regulatory environment and media-driven consumer awareness is finally driving capital to the rescue and it's showing up as smart, highly entrepreneurial, and funding innovation that is disrupting the likes of Cisco and IBM with value never before seen in the space. In just 2 years almost $4.6 billion of ambitious capital has come into cyber security start-ups and the increasing level of disruptive innovation is a significant and irreversible mega-trend that Florida is optimally positioned to take to the next stage for the advancement of the cyber security industry.

The real problem with cyber security in the U.S. and correspondingly the bigger opportunity for Florida is in correcting the terrifying levels of apathy we must deal with in mitigating the problem in the near and intermediate future. With the combination of having a nation snookered by a "free" internet economy (and

minting the youngest billionaires in history over the shortest periods of time) and the confiscation of our privacy and digital assets by sovereign powers, we have a very long way to go.

For more see "How to be a Billionaire by 30, the Arbitrage of Your Privacy." and "At the Leading Edge of Cyber Security as a Social Science."

- **Replace "Outreach" with "Distribution"** - Outreach is a soft word, and cyber security is a hard problem. Replace it with "Distribution". Distribute information, resources, and solutions to the capillaries of the Internet and personalize the issues where they matter most; at the individual level. There, awareness and behavioral adaptation take place and are brought back to the "system" for long-term ROI. Cyber security innovation is eliminating hardware and the requirement for local IT support. It is distributed electronically, is "smart", "aware", draws from collaborative intelligence, and is proactive and preemptive in its defenses. Increasingly, the only thing between optimal defense at the most vulnerable junctures and the real world of mainstream life is distribution, and Florida can play a leading role in figuring out the alchemy of making it happen.

- **Mine the Crisis in Florida for Cybersecurity Analytics and Digital Forensics** - Cybersecurity analytics and digital forensics are booming industries of the future and Florida has the perfect Petri dish for its R&D. No place else has the concentration of rich data Florida does, and the State, like our Internet billionaires (but with higher regards for privacy and personal information), should extract all of the value it can for the sake of economic monetization and playing a sustaining role in the growth of an industry. The first and hugely valid objection with this tactic concerns the lack of trust between private enterprise and government. We have to believe we can overcome by using time-proven structures and entities to narrow the divide, innovate new approaches to checks and balances, and constantly reverting the issue back to leadership.

- **Position State Resources at the Intersection of Cyber Risk Democratization and the Commoditization of Security Technology** - It's an awkward but uncomplicated sentence, so let's drill in. The Internet is now and will continue to push cyber risk to the furthest capillaries of the network, and the phenomenon is about to be seriously exacerbated by the IoT, or Internet of Things. The mega-trend is fueled by Moore's Law, but so is the mega-trend toward better, easier, faster, and cheaper solutions and this side of the equation is just raising its head. With an eye on the innovation, mostly software-defined, cloud-enabled, and deliverable "as a service" solutions, Florida can pump risk mitigators down the arteries for broad consumption and efficacy. The opportunity to open new markets by matching innovation with risk in its respective environments is enormous for Florida as it is in a position to develop and define the

intersection; where, how, and with what it takes place.

- **Create an Underwriters Laboratory for Cyber Security Technology -** The SUS, or State University System can be positioned as an Underwriter's Laboratory of the future. Here, infrastructure can be built to receive, test, and opine on new technology and the efficacy of its application toward cyber risk management and mitigation at its target market's environment. The opportunity for branding and licensing as an independent expert and resource is vast and holds potential for decades to come.

- **Target Seed Grants to Open Up and Lock Down -** With full credit to the nation's first CTO, Aneesh Chopra, we borrow the phrase "Open Up to Lock Down." Aneesh has a terrific presentation that harkens back to DARPA's Red Balloon Challenge of 2009. FC2, Enterprise Florida, the SUS, and other State level resources should deliberately mine the enormous levels of embedded innovative talent in Florida and the rest of the country by targeting seed grants outside of "the system". New thinkers, ones that are connecting dots that entrenched experts can't even see, are in our midst and hold answers that will drive progress toward effective resolution of the problem. As a classic example of the need to reach outside its easy to use Kodak as a case in point. Eastman Kodak invented the digital photo and owned its patents, but the multi-billion dollar company with 10's of thousands of employees could not see past their little yellow box of film and kept the innovation at a distance. Ironically, but true to form with disruptive progress, Kodak went bankrupt the same year Instagram was sold to Facebook for over $1 billion and nary a dozen employees. Florida must funnel seed grants to find the same magic of innovation and productivity to bring it to bear in their cyber risk management and mitigation problems, and opportunities. Finally, the mantle of "Opening Up" the public sector has broad, bipartisan vision and support and can be leveraged to tap federal resources for the sake of the cause to "Lock Down" on cyber security across the nation.

- **Act as a Conduit of Connectivity for the Emerging Collaborative Resources and Cyber Security Intelligence Around the World -** We have a long way to go but from Obama on down the vision is out there; share the intelligence for the sake of better preparedness and preemptive abilities. Florida can act as a model, at the tip-of-the-spear for the cause, and build systems and infrastructure that effectively collect and distribute the collaborative intelligence across the network. The issue requires new structures of partnership for trust and verification, but Florida can act as a leader to bring shape and lead the way toward implementation around the world.

- **Brand The Cyber State by Engaging Florida Government Agencies and Municipalities With the Cause -** Brand by leading with

example to engage cities, airport commissions, public libraries, and others to create cyber safe environments in their respective jurisdictions. Florida residents and visitors will be reminded the state takes the issue of their cyber safety seriously and when on public WiFi's, they are protected with state-of-the-science defenses engineered and operated by homegrown businesses and public sector partnerships.

- **Underwrite and Host an Annual "Disruptors Ball" Conference -** Florida can act as lead syndicator to underwrite an annual "Disruptors Ball" conference for hosting vendors, thought-leaders, investors, and industry visionaries in the area of cyber security technology and services, with a focus on broad, holistic and social applications of the science.

- **Partner with the Private Sector for Tech Transfer and R&D -** Experiment with the private sector by offering incentives to benefit mutually through trials and data collection exercises. For one example of which there are many, work with an enterprise to offer its employees cyber security as a benefit for their homes and families. Then collect data contrasting before and after compliance levels with awareness and behavioral application at the workplace. Measure the ROI, bank the intelligence, and move on. We wrote more about this specific approach here: "IT Security as an Employee Benefit."

Between IT security problems and solutions, opportunity abounds for Florida and its quest to be the nation's "Cyber State". The formidable energy between the two opposing yet aligned forces is mounting, and we hope played for all its worth.

Brad Deflin
Total Digital Security
President and Founder

West Palm Beach, FL