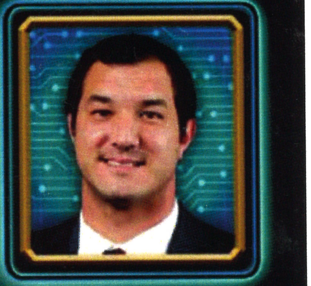
Florida Technology MAGAZINE

2024 Legislative Edition

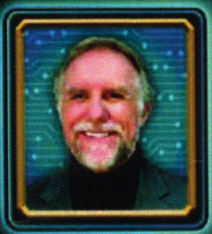
Senator
Jason Brodeur

Representative
Fiona McFarland

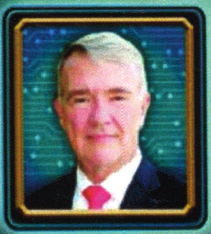
Representative
Susan Valdes



Representative
Mike Giallombardo



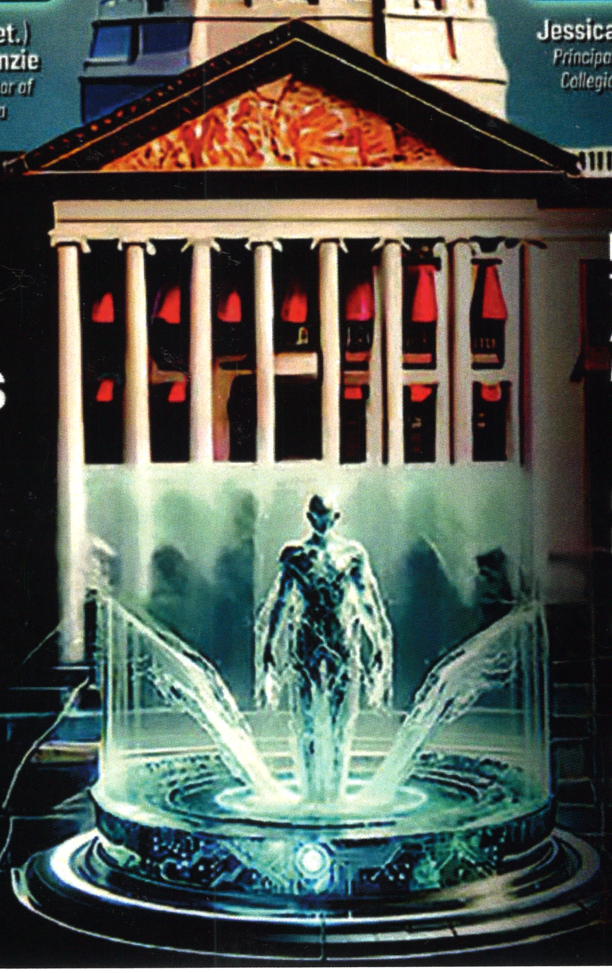
James Taylor
CEO of the Florida Technology Council



General (Ret.) Frank McKenzie
Executive Director of Cyber Florida

Jessica Chapman
Principal, Tallahassee Collegiate Academy

Tim Brown
Assistant Vice-President, ITS: NWRDC and FLVC at Florida State University



Why Harnessing AI in Florida's Agriculture Industry and Beyond is Important

Page 11

Empowering Tomorrow's Innovators: *A High School Blueprint for Future-Ready Students*

Page 4

Crafting an Effective Framework: *The Government's Role in Governing AI*

Page 20

Florida Establishes Master Credentials List

Page 35

Leadership-Driven Cybersecurity:

A Hillsborough County Case Study

*By **Kristan Keyes**, CGCIO, Director of Cybersecurity at Hillsborough County,* Information & Cyber Security Division, Office of the Chief Information & Innovation Administrator

Empowered by Leadership

The elevation of Hillsborough County's cybersecurity program is inextricably linked to the unwavering support and visionary leadership of the Chief Information and Innovation Administrator, Ramin Kouzehkanani. Under his guidance, we have cultivated an environment of autonomy, empowerment, and collaboration.

Expertise, Empowerment, and Unity

Our cybersecurity team is a testimony to the power of collective expertise. Supported by best-in-breed tools, we provide the team with the means to effectively combat evolving threats and maintain a high degree of situational awareness. Our leadership sponsors cross-training initiatives that ensures every member of our group possesses expert-level knowledge of each attack vector and the corresponding tools required for an effective defense. This training promotes resilience, fosters job satisfaction, nurtures deeper relationships, and cultivates an indomitable spirit. This unwavering unity demonstrates our commitment to security awareness, allows the team to swiftly navigate the complex cyber landscape, and empowers everyone to confront threat actors with tenacious determination in the face of sophisticated attacks.

Hillsborough County Digital Defense Sequence

Our advanced analytics suite, powered by MXDR (Managed Extended Detection and Response) and metrics-driven insights grants us unparalleled visibility into the evolving threat landscape. The

The Hillsborough County Cyber Security team has an exceptionally proficient and diverse team of professionals who possess a cumulative experience of over 100 years in the fields of technology, cybersecurity, infrastructure, cloud, and much more. The team is characterized by its extensive expertise and is well-equipped to tackle the multifaceted challenges of the cybersecurity and technology infrastructure domains.

Every member of our team holds some of the most prestigious and widely recognized certifications within the industry, ensuring comprehensive coverage across all aspects of cybersecurity and technology infrastructure, in addition to Department of Defense Top Secret clearances. These certifications serve as a testament to our commitment to staying at the forefront of the ever-evolving landscape of cyber threats and technological advancements. Our team's continuous pursuit of knowledge and skills development guarantees that we are well-prepared to safeguard the organization's digital assets and maintain the highest standards of security.

Here are some of the affiliations and certifications held by the team:

GISP · Federal Communications Commission · Department of Defense · CompTIA Network+
GMON · GDPR · CISA · CompTIA A+
GSEC · Microsoft Certified · InfraGard · CompTIA Security+
CISM Certified Information Security Manager · CCSK · hp · SANS · GCIH · Google Cloud Certified · Cisco Certified CCNA · EC-Council Certified CEH
CRISC Certified in Risk and Information Systems Control · CISSP Certified Information Systems Security Professional · ITIL · CompTIA INFOSEC · NIST · EC-Council
CGCIOFlorida · cisco · Google · (ISC)² · ISACA · CIO Executive Council

Hillsborough County Digital Defense Sequence (HDDS), our customized adaptation of the Lockheed-Martin cyber kill chain, is the foundation of our process. Recognizing that a single framework cannot guarantee absolute protection, we harness the HDDS in conjunction with a host of industry frameworks to proactively identify and address vulnerabilities, arming our defenses with the agility to adapt to ever-changing threat patterns.

We emphasize cyber hygiene practices, such as patch management and vulnerability scanning, to prevent incidents while network traffic monitoring identifies potential threats and anomalies. Prevention and detection drive our solutions and allows us to respond with minimal impact to the enterprise.

HDDS in Action: A Practical Example

An adroit cybersecurity engineer detected malicious activity emanating from a public network, leading to the discovery of a bad actor attempting to launch hacking tools. Our engineer immediately intervened, halting the execution of malicious tools, eradicating the threat from the device, and rebooting the compromised computer using industry standard recovery software, reverting it back to its pristine state. This incident highlights the effectiveness of our HDDS framework, cybersecurity team, and proactive threat mitigation tools.

Navigating the MoveIt Breach

In the wake of the MoveIt breach, our incident response team proved their worth, enabling us to navigate the situation effectively. Despite the nature of the attack and its widespread impact, our team demonstrated resilience and promptly contained the damage. As we move forward, we remain vigilant against third-party threats and continue to enhance our cybersecurity posture. We also extend our expertise to constitutional offices who do not have dedicated cybersecurity resources.

Preparing for PCI Version 4

As the PCI Data Security Standard (PCI DSS) prepares to transition to Version 4, Hillsborough County BOCC is at the forefront of compliance efforts. We are actively engaged in evaluating and implementing the new requirements, ensuring that our systems and processes align with the latest compliance standards.

By embracing this proactive approach, we are confident in our ability to safeguard our digital assets and protect the sensitive data of our constituents.

Aligning Our Incident Response with FL HB 7055

Our incident response plan is robust and aligns with leading practices and relevant guidelines, ensuring effective and coordinated response to cybersecurity incidents. It seamlessly integrates with FL HB 7055, NCIRP, and NIST Cybersecurity Framework for Resilience. This approach ensures that our response efforts are aligned with state-level, federal, and international standards, maximizing our effectiveness in addressing cybersecurity threats.

Maximizing Resources, Minimizing Risks

Deep examination of our existing budget and leveraging opportunities presented by grants, we have achieved significant milestones in strengthening and building upon our cyber posture. We approach information security and risk management with the utmost fiscal responsibility.

Our approach of 'efficient resource utilization' is not merely a catchphrase; it's an essential strategy in the ever-evolving cybersecurity landscape. We acknowledge the elusive nature of absolute security and constantly refine our methods to enhance our resilience. However, additional resources would undoubtedly strengthen our existing protective measures.

Hillsborough County Shares Best Practices

Hillsborough County actively engages with fellow Florida CIOs to share best practices (HDDS) and foster a collective cybersecurity posture. This collaborative approach strengthens the state's defenses against cyber adversaries. A more secure digital landscape also translates into a benefit for taxpayers through reduced costs associated with cyberattacks.

In the face of ever-evolving cyber threats, no single organization can stand alone. By working together, sharing knowledge, and strengthening our collective defenses, we can create a more resilient digital ecosystem that safeguards the well-being of our residents and paves the way for a brighter future.