

Energy, Communications & Cybersecurity Subcommittee

Tuesday, January 17, 2023
2:00 PM - 4:00 PM
Reed Hall (102 HOB)

Meeting Packet

Paul Renner
Speaker

Mike Giallombardo
Chair

The Florida House of Representatives

Commerce Committee

Energy, Communications & Cybersecurity Subcommittee

Paul Renner
Speaker

Mike Giallombardo
Chair

Meeting Agenda

Tuesday, January 17, 2023
2:00 PM – 4:00 PM
Reed Hall (102 HOB)

I. Call to Order

II. Roll Call

III. Welcome and Opening Remarks

IV. Presentation on the 2022 Cyber Attack on the Highlands County Sheriff's Office

V. Overview of the Florida Digital Service

VI. Closing Remarks

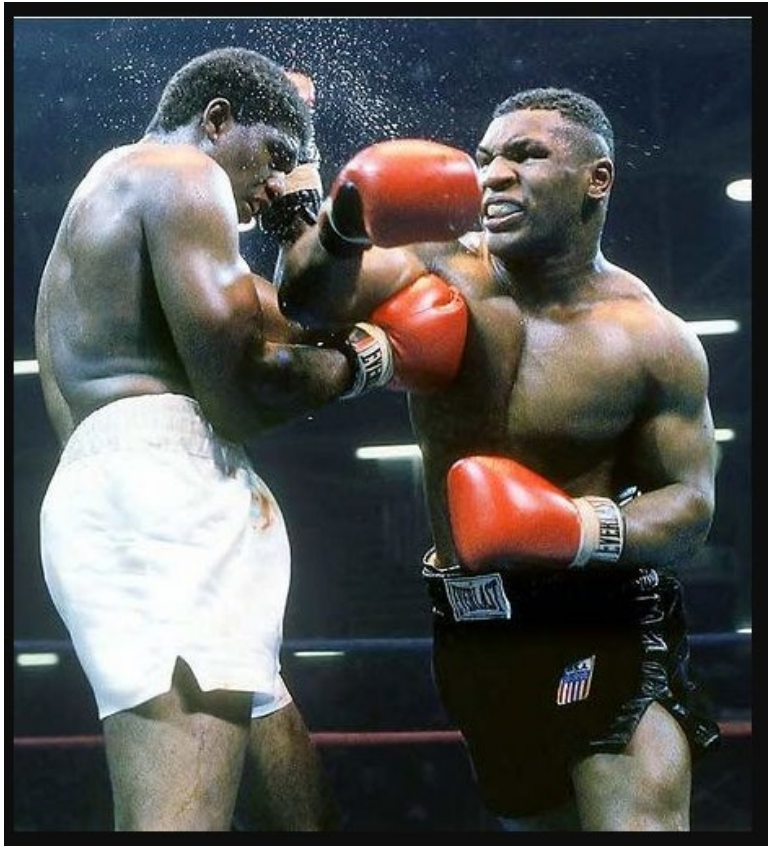
VII. Adjournment

RANSOMWARE ATTACK

Garrett S. Roberts, General Counsel

“EVERYONE HAS A PLAN UNTIL THEY GET PUNCHED IN THE MOUTH.”

-Mike Tyson



What Is Ransomware?

"A type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return."

- FBI definition



Attack on the Highlands County Sheriff's Office

May 10, 2022

Ransomware actor was able to embed software to allow a reconnaissance mission weeks before the actual attack. This is the typical strategy utilized by ransomware actors to give them time to analyze the system.



Attack on the Highlands County Sheriff's Office

May 11-26, 2022

Reconnaissance of entire network to ensure they knew exactly how to hit our system to cause the most damage. During this time, the ransomware actors were able to obtain administrator credentials to our network.



Attack on the Highlands County Sheriff's Office

May 26, 2022

At approximately 11 p.m., an employee in the jail noticed an issue with our computer network and notified a member of the IT Unit. He quickly realized this was not a typical computer issue. This was on a Thursday night before the start Memorial Day weekend.



Attack on the Highlands County Sheriff's Office

May 26-27, 2022

Despite immediate steps being taken to isolate our network systems, the damage had been done. A significant portion of our data had already been encrypted and the entire system had to be taken offline. Our supposedly secure network backup had been completely erased.



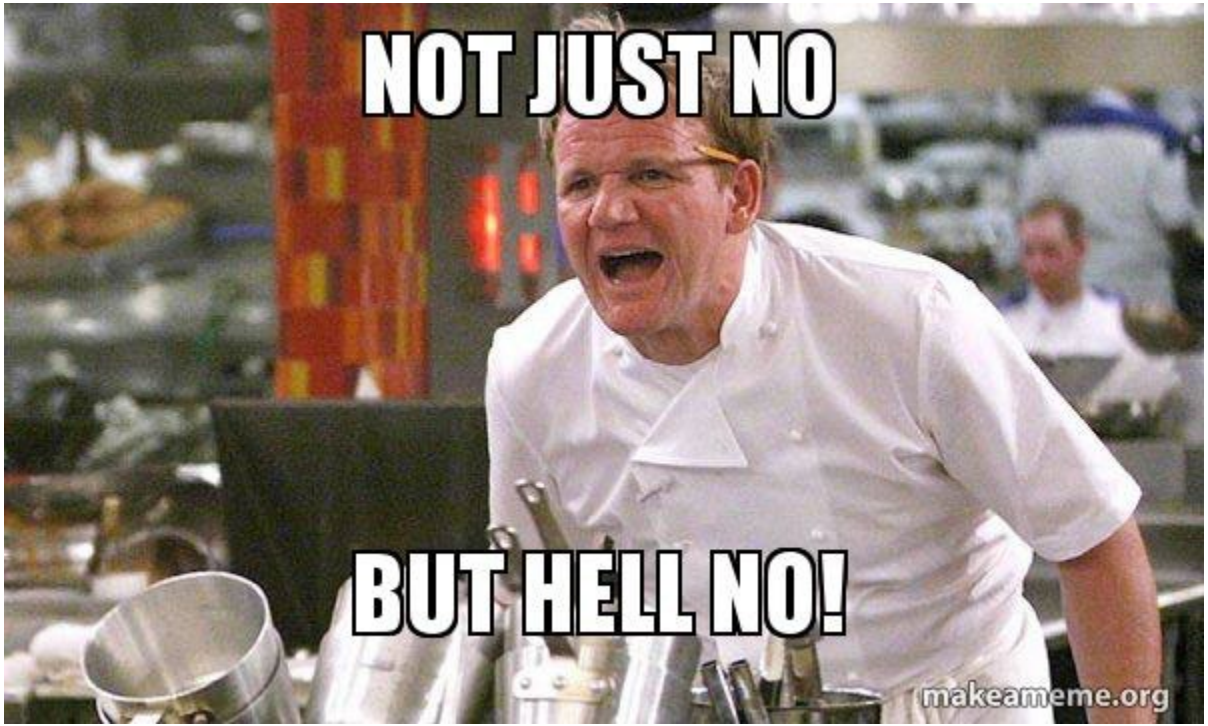
Ransom Demand

Now that they had our attention …

When contact was made with the attackers, they demanded we pay them $2.5 million in Bitcoin in order to receive the key to decrypt the data they now held hostage.



Our response …



Significance of a Ransomware Attack on a LE Agency

Types of sensitive data that a law enforcement agency has stored in its computer network:

- Social Security numbers
- Dates of birth
- Driver License information
- Current and past addresses/phone numbers
- Medical Examiner reports
- Victim information
- Criminal history
- Investigative information
- Employment records
- Information on employees' family members
- Medical information on employees and inmates
- Polygraph results
- Psychological test results

What to Expect Immediately After an Attack

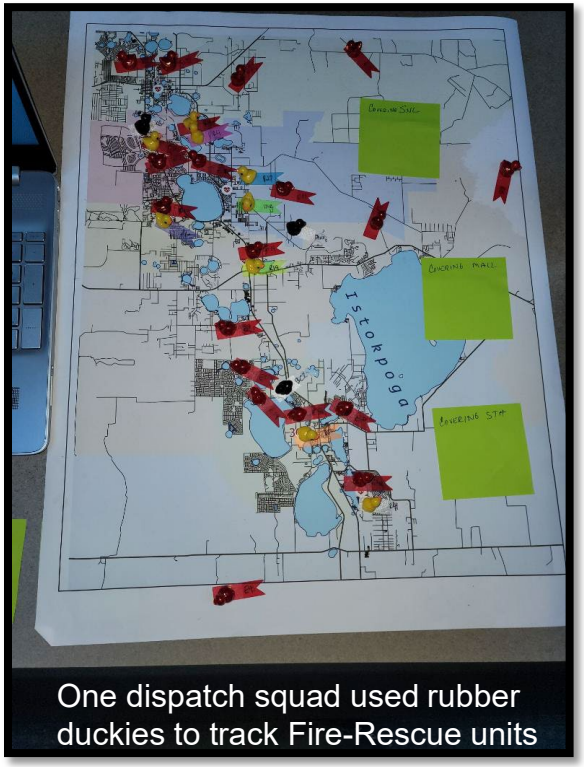
- Panic by members
- Rumors spreading
- No VOIP phones
- No computer access
  - Dispatch
  - Law Enforcement
  - Detention
  - Administrative

- No cameras
  - Jail security
  - Main building security
  - ALPR
  - In-car or body cams



Operational Considerations – Law Enforcement

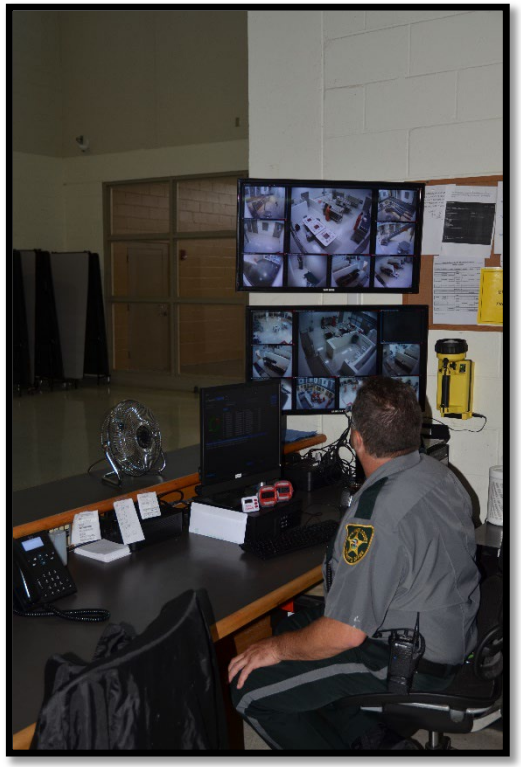
- Computer Aided Dispatch (CAD) will not be operational.
- FCIC/NCIC will not be accessible.
- Dispatchers will be using paper notes and maps.
- Deputies will be filling out reports by hand.



One dispatch squad used rubber duckies to track Fire-Rescue units

Operational Considerations – Detention

- Jail booking software will not work.
- Inmate classification records will be inaccessible.
- Security cameras will be inoperable.
- Calendars (court appearances, release dates, etc.) not available.
- Medical unit will not have access to records or medication plans.



Operational Considerations – Agency-wide

Data loss could occur in any (or all) of these areas of your agency:

- Training records – state certifications, specific training certificates
- Evidence – property receipts, etc.
- Criminal cases
- Cold Cases
- K-9 records
- Fleet records
- Animal Control
- Capital Property Inventory
- Accreditation records required
- Finance (information not available to complete a fiscal audit)
- Payroll
- Agency website



Public Relations Concerns

Make sure your employees have all information before the public

- Work with Public Information Officers to develop talking points.
- Release an initial statement as soon as possible in order to ensure correct information is available and prevent rumors.
- Be as transparent as possible.
- Reassure public that someone will answer the phone when they call and that deputies will still come.
- Ask the public to be patient as you work through the initial phase and develop workarounds.
- Release follow-up messages when there is new info.



Key Take-Aways – Strategic Operational Plan (Law Enforcement)

- Prepare fillable PDF copies and hard copies of all incident/arrest reports, property receipts and any other often-used forms. Store files on a separate device (thumb drive, isolated external hard drive, etc.).

- Have a plan to utilize a numbering sequence that will enable proper sequencing once CAD is operational.

- Have a plan in place on how to collect reports and prepare them for release in response to public records requests.

Key Take-Aways – Strategic Operational Plan (Detention)

- Prepare to book inmates using paper and/or a laptop.
- Prepare to have proper staffing in areas where cameras would typically cover for safety of staff and inmates.
- Have a plan on how to release inmates. There is significant liability for holding inmates past their release date.

Key Take-Aways – Strategic Operational Plan (Admin.)

- **Have Insurance:** You will need significant highly specialized resources as soon as an attack occurs. Our insurance policy (through the FUND) enabled our agency to have resources within hours of the initial attack:
  - Forensic computer analysts
  - Computer software
  - Ransomware negotiators
  - Privacy attorney

- **Your payroll software will be inaccessible:** The first concern your employees will have is whether they are going to be paid. Many people live paycheck to paycheck.

Key Take-Aways – Summary



Prepare for at least several weeks and maybe months back in the 19

Liability Concerns

- **Class Action Lawsuit:** Filed by effected individuals whose information has been released. This will likely be 100,000 or more individuals for a law enforcement agency.
- **Fines & Penalties:** OFAC & Treasury Dept. if payment to someone of prohibited list.
- **Fines & Penalties:** if you fail to comply with Federal and State reporting requirements.

Final Point

- **Stress test your system:** Just because your IT Department ensures you that your system (and backup servers) are “impenetrable” does not mean you are safe. Our “secure” backup server was completely wiped.

- Utilize third-party resources (“white hat hackers”) to seek vulnerabilities in your system.



Florida [Digital Service]

CYBERSECURITY OPERATIONS

2023_JANUARY

Enterprise Cybersecurity Program

- FL[DS] serves as the lead state entity on cybersecurity. 282.318, F.S. directs the Digital Service to:
  - Operate and maintain a Cybersecurity Operations Center led by the State CISO, including a process for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.
  - Detect threats through proactive monitoring , continuous security monitoring, and defined detection processes.
  - Establish incident response teams.
  - Recover information and data in the event of a cybersecurity incident.
  - Establish managerial, operational, and technical safeguards for protecting state government data and information technology resources, including establishing standards and processes for assessing state agency cybersecurity risk.

Individual State Agency Responsibilities

- Section 282.318(4), F.S. includes requirements of each agency, including:
  - Designate an Information Security Manager (ISM), coordinate cyber training.
  - Establish an agency cybersecurity team to respond to an incident and immediately report all confirmed or suspected incidents to the State CISO.
  - Conduct, and update every 3 years, a comprehensive risk assessment, to determine the security threats to the data, information, and IT resources.
  - Submit annually by July 31, strategic and operational cybersecurity plans.
  - Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended to address identified gaps in data, information, and information technology resources of the agency.
  - Develop a process for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents which is consistent with security rules, guidelines, and processes established by the Florida Digital Service.

The Current Posture

Positive Increase / Decrease

Negative Increase / Decrease

No Change

FLDS:

- Number of FTE: 70
- Cybersecurity FTE: 29
- Total FY 2022-2023 Appropriation: $148.2M
- Total FY 2022-2023 Cybersecurity Appropriation: $62.2M

Agency Collaboration:

- Number of Agencies which had ever collaborated in real-time on cybersecurity prior to FLDS: 0
- Number Currently Collaborating in real time on cybersecurity with FLDS: 32
- Number of Agencies Fully Integrating with the CSOC: 9
- Number of Agencies Partially Integrating the CSOC: 23



The Current Posture

Positive Increase / Decrease

Negative Increase / Decrease

No Change

High Level Threat Data

- Total Threat Sightings for the 6 agencies which have completed the Phase 1 integration with the CSOC : >2 Million ↑
- Total Investigations Currently Open: 172 ↑
- Open Investigations per FLDS FTE: 2.45 ↑
- Open Investigations per Cybersecurity FTE: 5.93 ↑
- Threat Sightings per FLDS FTE: 28,571 ↑
- Threat Sightings per Cybersecurity FTE: 68,966 ↑

Florida's First Cybersecurity Operations Center

Developing Security Capabilities from the Ground Up

Three Predominant Program Designs:

1. Single-Stack : procuring a standalone solution to operationalize all capabilities which eliminates dependence on third party integrations but limits product options.
2. Systems Integrator: procuring a single vendor to run the initiative and outsource all technology decision making to that vendor to determine design, architecture, and product roadmap (i.e., Deloitte, Accenture, KPMG, etc.).
3. Multi-Vendor Integrated Marketplace: a modular approach that supports numerous vendors and integrates multiple solutions.

FL[DS] selected #3 as the design for the CSOC for the following reasons:

- Establish a single point of ingestion, translation, and access for cybersecurity data.
- Avoid single vendor dependence.
- Provide access to the best solutions for each function.
- Avoid requiring agencies to adopt a single technology stack for all necessary functions.
- Preventing agencies from having to rip and replace certain solutions already deployed.

Ending the Siloed Approach to Security

FL[DS] began by focusing on two very real threats to the enterprise:

1. Zero state agencies were sharing security data or collaborating in real time on cybersecurity.
2. Unsupported and unsecured versions of Microsoft Office were being used prominently across state government.

FL[DS] offered to fund solutions to all state agencies. Initially, 21 of 36 state agencies opted to participate:

- FL[DS] funded cloud-based Microsoft Office Suite, including cloud-based email.
- Third-party, private sector implementation services, included at no additional cost to the taxpayer.
- Microsoft included engineering support post-implementation at no additional cost to the taxpayer.
- FL[DS] generated significant savings by purchasing as an enterprise which saved 25% ($4M) above and beyond state term contract.

FL[DS] has committed to provide these solutions to 7 additional enterprise entities which have opted in.

Florida's First CSOC
Launching the Core Functionalities

Building upon the focus on eliminating unsupported and unsecure productivity software, **FL[DS] deployed the core functionalities of a Cybersecurity Operations Center** including:

- **Asset Discovery** to identify and inventory enterprise technology resources:
  - Agent-based solution focused on infrastructure and supported with Managed SOC Services.
  - Agentless solution focused on network traffic and supported with managed services.
  - Internet-facing attack surface discovery.
- **Endpoint Detection and Response** to provide comprehensive and complimentary enterprise support.
- **Managed SOC Solution and Services** software which integrates all other incorporated solutions and supported by 24/7/365 Managed Security Services.
- **Content Delivery Network** to manage and secure enterprise web assets, both .com and .gov.
- **Training** Cyber range infrastructure and curriculum to support cybersecurity training and skill development.
- **Licensure and Credential Access** FL[DS] proof of concept to explore workstation licensure and credential management to ensure efficient offboarding of employees.

Quantifying the Threat Landscape

Current as of January 1, 2023

Positive Increase / Decrease

Negative Increase / Decrease

No Change

Asset Discovery: External View

- Total On-premise Assets Discovered: 961,386
- Total Cloud Assets Discovered: 9,018
- Open/Critical Issues: 4,030 / 274
- Top Threat: Insecure Web Servers (56)

Asset Discovery: Network Sensors (last 30 days)

- Discovered Devices: 360K
- High Risk Devices: 13.4K
- Threat Activity: 5,600 Events

Asset Discovery: Endpoint Sensors (last 30 days)

- Endpoints w/ Agent Installed: 6,242
- Discovered Devices: 10,683
- Devices Missing Patches: 6,578 (301 Critical)

Endpoint Detection and Response (30 Day Lookback):

- Resolved Incidents (30 days): 190
- Threats Detected (30 Days): 192
- Malicious Threats Mitigated (30 Days): 39
- Closure Rate Prior 30 Day Period: 99.68%
  - 30 day period prior was 83.52%
- Current Closure Rate: 98.95%

Content Delivery Network (30 Day Lookback):

- State Websites Actively Protected: 51
- Attack Traffic Diverted: 6.4 Million Events (e.g., Botnet, DDoS)

Challenges and Solutions

Cybersecurity Challenges

- Starting from Scratch
  - $100+ billion dollar enterprise that has never previously done enterprise cybersecurity
- Workforce
  - Affording and Recruiting the Talent Necessary to Build and Operate Across the Enterprise
- Volume of Threats
  - Number of threats which would have to be cleared per FLDS each day to resolve known existing threats in a year, assuming no additional threats are discovered (260 workdays): 7,692

FL[DS] Solutions

- Starting from Scratch
  - Establishing the baselines and implementing the fundamentals
  - Maintaining an agile posture as much as bureaucracy allows
- Workforce
  - Tour of Service Model
    - CISO: 10+ year IBM cybersecurity and active Naval Reservist: USCYBERCOM
    - Deputy CISO OPS: 20+ Air/Space Force Cyber Warfare Officer, 2+ Years Private Industry Cybersecurity
    - Deputy CISO Strategy: 8+ Years as Agency CIO Leading Digital Transformation and Security Efforts
- Volume of Threats
  - Automating Everywhere Possible
  - Leveraging Private Sector Managed Services to Augment FLDS FTE in a Hybrid Workforce Model

Cyber Security Updates:
Strategy and Planning – 2022 Review

- **CSOC launched**
- **State Incident Response Plan Published**
  - **Living document to support state and local entities needing to report a cybersecurity incident to facilitate incident response**
- **Launched Cyber Range training capabilities with real-time blue team training for security professionals to respond to an active intrusion or attack.**
  - **20+ agencies have either run or are scheduled to run exercises since September 2022 on the Cloud Range platform**
- **Established Statewide Cybersecurity Strategic Plan:**
  - **Redesigned FL enterprise security by taking the approach of a partner vs an enforcer.**
- **Updated Agency Cybersecurity Strategic and Operational Plan (ASOP) process to align to the Statewide Cybersecurity Strategic Plan:**
  - **Rebuilt antiquated ASOP process, reduced time agencies had to spend preparing the plan by 75%.**
- **Established quarterly Incident Response reporting to map trends in enterprise security**

Building Upon the Success in 2022

Expanding the Program's Capabilities

- Acquire and deploy a Governance Risk and Compliance software suite
- Provide Identity and Access Management solution(s) for the enterprise
- Provide Multi-factor Authentication solution(s) to the enterprise

"Whole of State" Cyber to Extend the Reach of the Program Beyond State Government

- $30m to deploy cybersecurity capabilities to local government entities through a competitive grant program
- Expand cybersecurity training opportunities to state and local entities
- Develop and publish 2023 Statewide Cybersecurity Strategy
- Review and update reporting method for Agency Strategic and Operational Cybersecurity Plans
- Expanding the FIRE Team Footprint to increase incident response times and effectiveness



Questions?