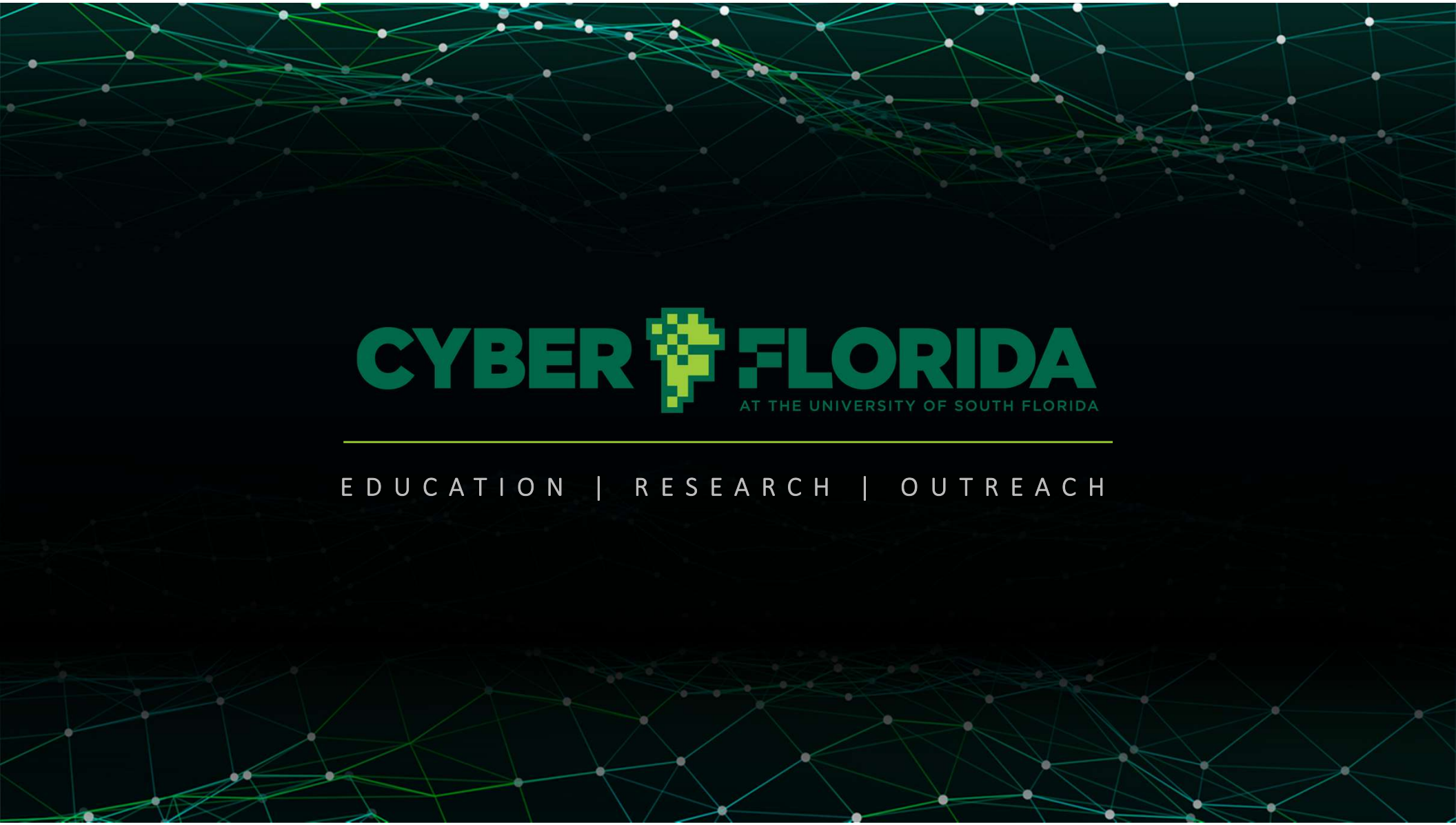

CYBER FLORIDA
AT THE UNIVERSITY OF SOUTH FLORIDA
EDUCATION | RESEARCH | OUTREACH

On Behalf of Cyber Florida…

About Me

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM
POWERED BY CYBER FLORIDA at USF

Emeka Okammor

Cybersecurity Resource Manager

Contact Information:

EmekaOkammor@CyberFlorida.org

- University of Central Florida, M.S. Management Information Systems (M.I.S.)
- 14 years in Cyber Security
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)

UCF KNIGHTS

CISSP® Certified Information Systems Security Professional

CISA® Certified Information Systems Auditor® An ISACA® Certification

Who Are We?

Established in 2014: FS 1004.444 Make Florida "the national leader in cybersecurity"

Education Build/expand cybersecurity workforce development

Research Enable/expand cybersecurity research capabilities across the state and enable technology innovation

Community Outreach and Engagement Engage communities to raise cyber-awareness and resilience

Cybersecurity Public Policy Shape public policy to enhance cybersecurity across the state.

Operation K12 Cybersecurity career preparation of Florida education system

Outreach & Events Public awareness campaigns and events to help vulnerable organizations enhance their cybersecurity

SOCAP: Security Operations Center Apprentice Program Hands-on experience to complement degree programs

CyberLaunch Florida's statewide high school cyber competition

What Are We Doing?

GRANT-FUNDED & STATE INITIATIVES

Florida's Cybersecurity Critical Infrastructure Risk Assessment

Conduct a voluntary cybersecurity risk assessment for Florida-based public and private critical infrastructure organizations

Statewide Cybersecurity Training Program

Provide cybersecurity awareness and training courses tailored to job roles for all public-sector employees

Cyber Range (HB 5001)

Provide a cost-effective, realistic cybersecurity training environment for city, county, and local governments

CyberWorks: Cybersecurity Workforce Development (NCAE)

Prepare veterans and transitioning first responders for jobs in cybersecurity

CYBER FLORIDA FIRSTLINE

No-cost education & training for Florida's public sector

$30M in non-recurring funding from the Florida Legislature to provide no-cost cyber education and training to every Florida state, county, and municipal government employee

University of South Florida:

- 4- to 8-hour classes for executive, managerial, and general staff
- 4-week industry certification prep courses for technical roles
- A handbook for state and local government employees
- Mostly virtual (synchronous and asynchronous)

University of West Florida:

- 1- to 8-week industry certification prep courses for technical roles
- Mostly virtual (synchronous and asynchronous)

Florida International University:

- 8- to 16-hour classes for executive, managerial, and general staff
- FIU experience indicates in-person attendance is the most desired mode for this audience
- FIU partnered with 7 institutions across the state to minimize travel while providing more in-person sessions

UNIVERSITY of SOUTH FLORIDA

CENTER FOR CYBERSECURITY AT THE UNIVERSITY OF WEST FLORIDA

FIU FLORIDA INTERNATIONAL UNIVERSITY

NW3C

NCCARI 1819

powered by CYBER FLORIDA AT USF + SIMSPACE

ARCS RANGE

ALIGNED REALISTIC CYBERATTACK SIMULATION RANGE

RANGE FEATURES

- Florida County and Local government IT and OT cybersecurity personnel - public sector focused
- Cyber Range as a Service (CRaaS), 100% cloud-based training model
- No cost for public sector users
- Supports Statewide Training Program

KEY MILESTONES

- Launched March 2024: SimSpace selected as vendor; soft launch
- Currently 145 users across 17 counties on ARCS Range

SOCap

Security Operations Center Apprentice Program

Provides hands-on cyber threat monitoring, digital forensics, and reporting skills for up to 20 USF students each year

SERVICES OFFERED/STUDENT LEARNING OBJECTIVES

- Hands-on experience for students to bridge the gap between academia and work experience
- Students learn state-of-the-art real-time cybersecurity monitoring and threat detection tools
- Cybersecurity services include
  - Digital forensics, including enterprise and mobile devices
  - Incident response (remote triage assistance)
  - Malware analysis, Log management and review
  - Log collection and analysis
  - Cybersecurity projects, assessments, and consulting
  - Coming soon: vulnerability assessment and penetration, and testing

CyberWorks
workforce development training

- Grant-supported
- Industry partners include JPMorgan Chase, ReliaQuest, KnowBe4, Amazon Web Services, VMWare, Rapid7, Cisco, Raytheon, OPSWAT, GuidePoint

- **NICE Work Role:** Cyber Defence Analyst
- **Enrollment:** Two cohorts per year, 30-40 students per cohort
- **Courses/Badges:** Network Fundamentals, Cyber Defense Fundamentals
- **Industry Certifications:**
  - CompTIA Network+
  - CompTIA Cybersecurity Analyst (CySA+)
  - CompTIA Security+

OPERATION K12
POWERED BY CYBER FLORIDA

- Youth Engagement
- Educator Professional Development
- Curriculum Development

PROGRAM HIGHLIGHTS

- Active in districts across Florida through a tiered support system, as well as several other states, territories, and even countries
- Cybersecurity Essentials Course (including lesson plans, presentations, labs, tests, and activities) preps for industry certification exam
- CyberHub virtual lab environment provided at no cost
- Speakers Bureau, monthly webinars, Slack channel w/150 users
- Collaboration Center housed in Canvas provides curriculum guides, demos, exam prep, career resources
- Second Annual CyberLaunch Statewide High School Competition 4 April 2025

- Free online cyber risk assessment funded and authorized by the State of Florida
  - Entry-level assessment (20 questions) to identify vulnerabilities
  - Mid-level assessment measuring against the Cybersecurity Performance Goals (CPG)s
- Develop a Florida-Specific Cybersecurity Maturity Index/Model for critical infrastructure providers (MS-ISAC)
- Free resources for public and private sector critical infrastructure organizations, such as incident response plans, resource mapping, etc.
- Close the maturity gap for “basic” ransomware readiness
- Mapping tool (Cyber Bulls-I) to provide summaries for critical infrastructure cybersecurity initiatives using AI to map NIST 800-53 to all 106 CSF question
- Construct and maintain a comprehensive list of critical infrastructure entities operating in the state for sampling and communication purposes (intel sharing)

What is Cyber Bulls-I

Background to Cyber Bulls-I

The purpose of this solution is to help stakeholders in all 16 critical infrastructure sectors in Florida enhance their cyber posture by offering them a portal to track their current state and access resources based on NIST SP800-53 to close security gaps. The project objectives are to create a portal for respondents to complete their assessments, and access personalized resources offered by Cyber Florida to mitigate security weaknesses.

CYBER FLORIDA
AT THE UNIVERSITY OF SOUTH FLORIDA

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

Module Question: RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared

Cybersecurity Plan Questions

Please answer the following questions. The resources below should help you understand how to answer the questions. Then, click *Next Module* or download all of your certification answers.

What is your organization's name? Cyber Florida Lake Show

Who will identify critical 3rd party suppliers and external partners (Name and contact)? LeBron James

Download Plan Templates | Next Module

Resources to help you complete module RS.MA-01

Creating and executing an incident response plan with third-party coordination involves several key steps:

1. Establish the Plan

Develop a response plan that integrates your business continuity strategies and outlines roles, compliance requirements, and communication protocols. Update it regularly to reflect changes in the organization[12].

Module Question: RS.MA-02: Incident reports are triaged and validated

Cybersecurity Plan Questions

Please answer the following questions. The resources below should help you understand how to answer the questions. Then, click *Next Module* or download all of your certification answers.

Who is your incident command manager (Name and contact)? Anthony Davis

Download Plan Templates | Next Module

Module Question: RS.MA-03: Incidents are categorized and prioritized

Cybersecurity Plan Questions

Please answer the following questions. The resources below should help you understand how to answer the questions. Then, click *Next Module* or download all of your certification answers.

Who is your information technology/operational technology specialist (Name and contact)? JJ Redick

Download Plan Templates | Next Module

Module Question: RS.MA-04: Incidents are escalated or elevated as needed

Cybersecurity Plan Questions

Please answer the following questions. The resources below should help you understand how to answer the questions. Then, click *Next Module* or download all of your certification answers.

Who will create your cybersecurity incident reporting procedure (Name and contact)? Luka Doncic

Download Plan Templates | Next Module

Governing laws, regulations and guidelines

Source	Regulation/Section
The Florida Senate	CS/HB 7055: Cybersecurity
NIST	NIST SP 800-61, rev 2

Policy statements

Incident handling capability

Cyber Florida Lake Show will develop and implement incident-handling capabilities to cover all information system components that fall within the scope of this policy. The incident handling capability will include a defined plan and procedure to handle all stages of cybersecurity incidents: preparation, detection, analysis, response, containment, and recovery.

Organizational roles and authorities

Cyber Florida Lake Show will define the organizational cybersecurity structure, roles, responsibilities, and levels of authority to handle cybersecurity incidents.

Incident reporting responsibility

Cyber Florida Lake Show will track, document, and report incidents to appropriate authorities as required by governing laws and regulations.

Prioritization and severity ratings of incidents

Cyber Florida Lake Show will define how it will assign a severity rating to cybersecurity incidents to critical cyber services and prioritize them for response and recovery.

Adopt and implement a cybersecurity risk management framework

Directly responsible individual (Name and contact): Anthony Davis

A Risk Management Framework (RMF) integrates security into the organization's business processes. The framework allows organizations to select the most effective security controls within the organization's budgetary and regulatory constraints. As a baseline, the NIST risk management framework (https://csrc.nist.gov/projects/risk-management/about-rmf) can be used as a starting point. Typically, the CISO or designee is responsible for selecting the risk management framework.

Identify critical suppliers and external partners

Directly responsible individual (Name and contact): LeBron James

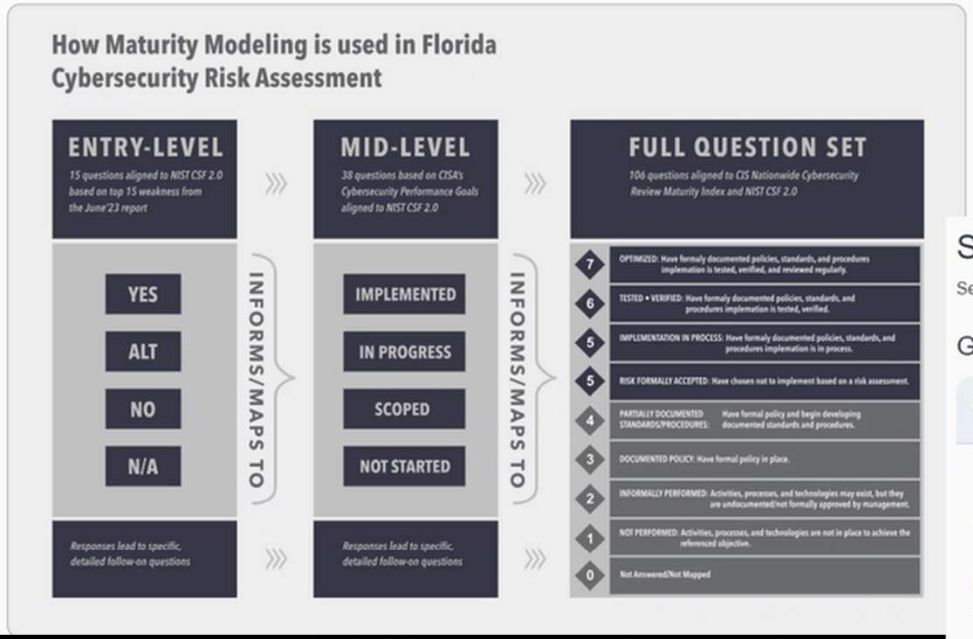
Suppliers, their supply chains, and their products or services are a potential source of harm to critical cyber infrastructure. For example, a compromised device at an air-conditioning service company can insert malicious code into the organization when the compromised device connects to the organization's network to repair a defective AC unit. Important suppliers and external partners should be included in incident response planning. Typically, the purchasing organization is responsible for identifying critical suppliers and external partners.

Volunteer Opportunity…

Conversion Tutorial

This assessment has been converted to a mid-Level assessment. Answers from the Entry-Level factor into the Mid-Level pre-filled answers. Answers from the Mid-Level factor into the Full pre-filled answers.

Below is a diagram for how the answers from one level impact the next:



assessment + NIST 2.0)

Standard Requirements

Select the applicable answer for each of the following questions. Unanswered questions are calculated as a 'No' response.

Govern - CSF 2.0

Organizational Context

GV.OC-01 The organizational mission is understood and informs cybersecurity risk management

0 1 2 3 4 5 5 6 7
Not Mapped — Optimized

0 - Unanswered / Not Mapped

This question has not been answered. Move the slider to answer the question.

GV.OC-02 Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered

0 1 2 3 4 5 5 6 7
Not — Optimized

5 - Implementation in Progress

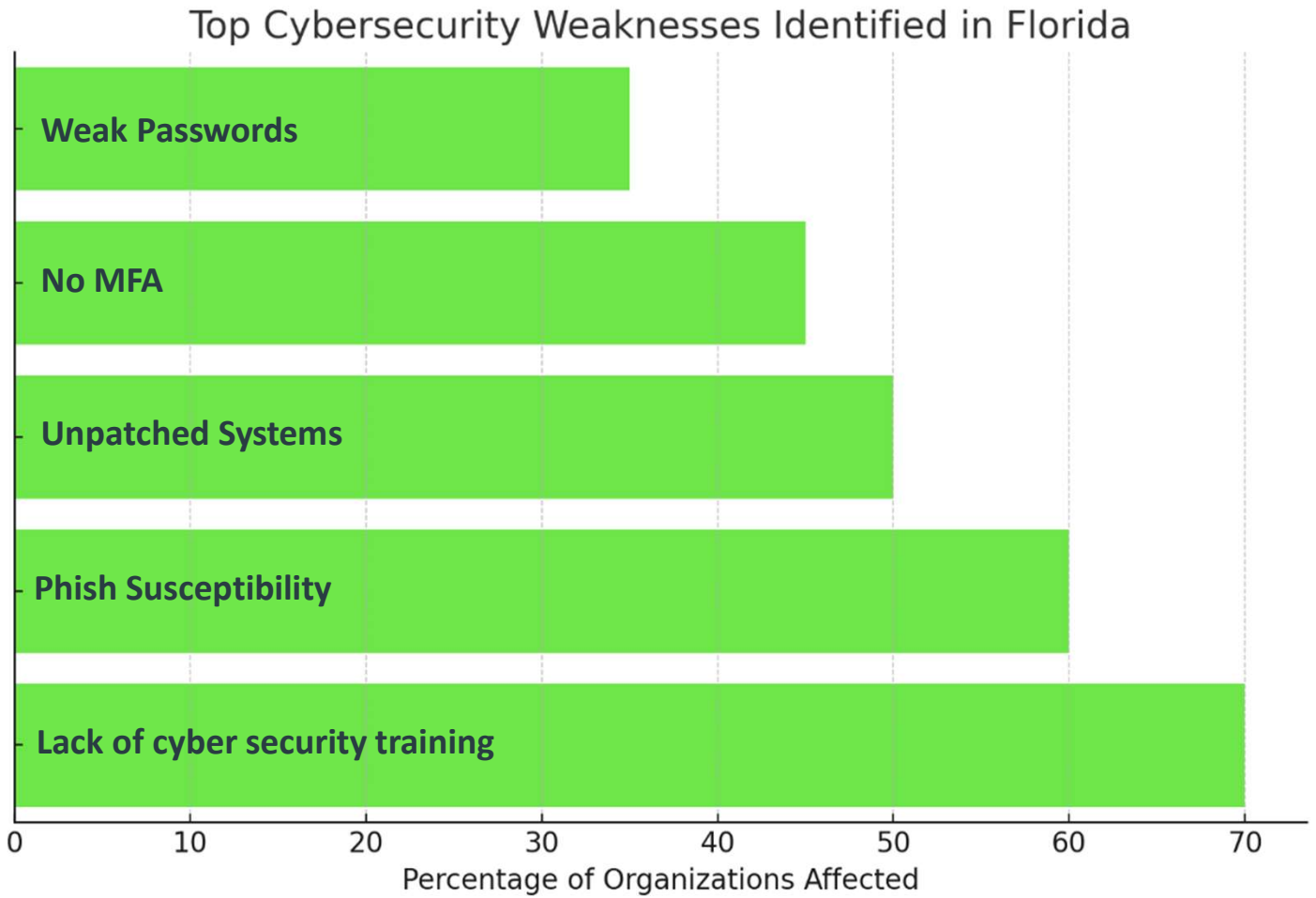
Your organization has formally documented policies, standards, and procedures and is in the process of implementation.

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

POWERED BY CYBER FLORIDA at USF

Trends and Findings

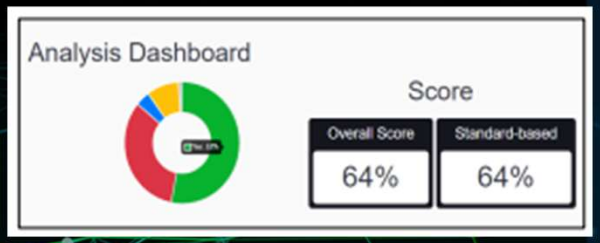
- 45% do not use multi-factor authentication (MFA)
- 50% do not test response and recovery plans with third parties, vendors, contractors, suppliers.
- **49%** of respondents do not have a Chief Information Security Officer (CISO)
- 59% of participants have between 11 to 500 employees.
- 7 out of 10 weaknesses are in Risk Management

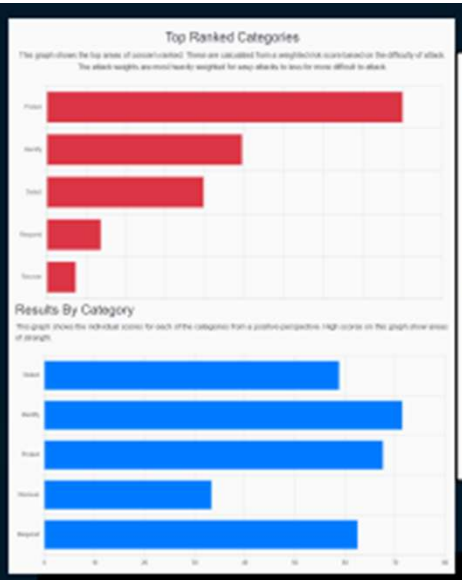

Top Cybersecurity Weaknesses Identified in Florida
Weak Passwords
No MFA
Unpatched Systems
Phish Susceptibility
Lack of cyber security training
0
10
20
30
40
50
60
70
Percentage of Organizations Affected

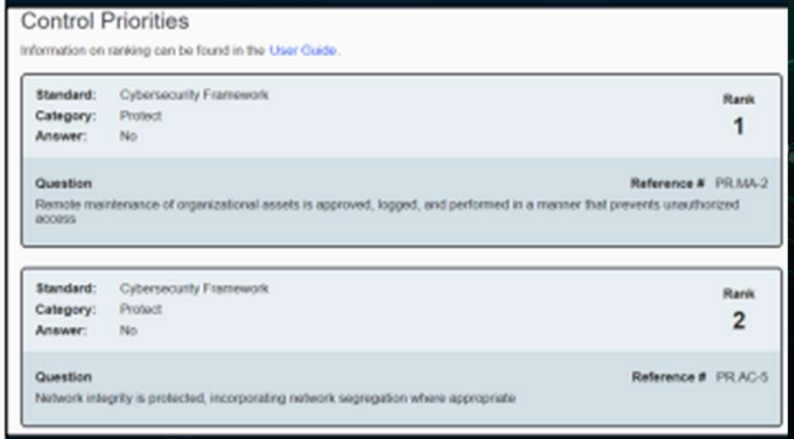
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

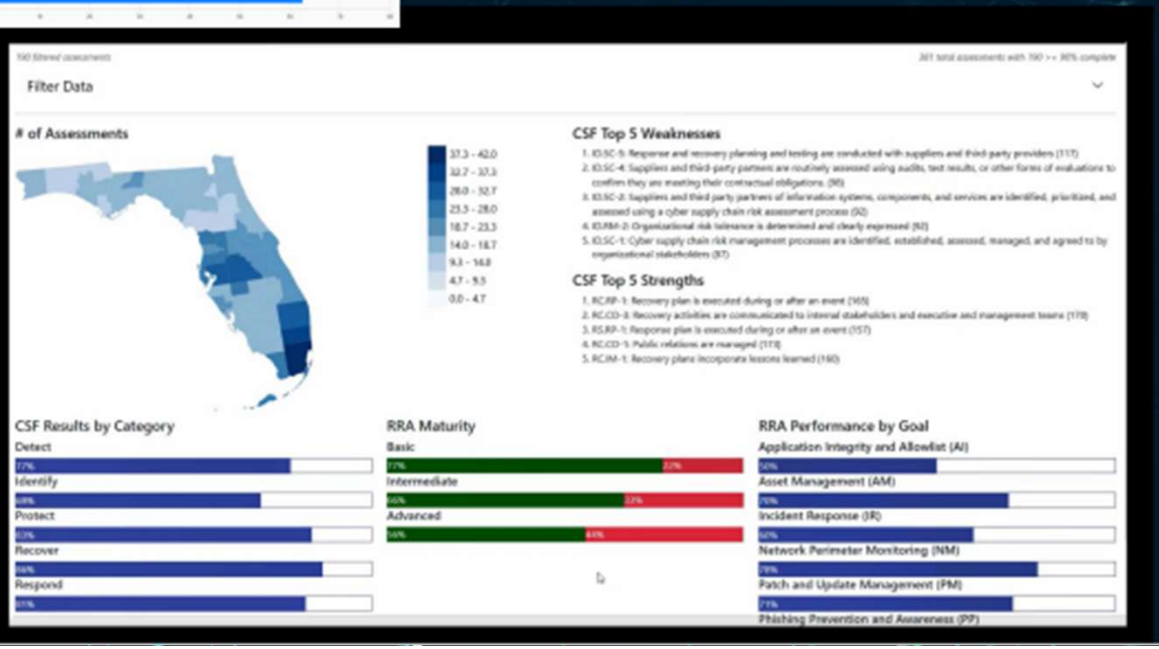
POWERED BY CYBER FLORIDA at USF

Critical Infrastructure Cybersecurity Risk Assessment Reports







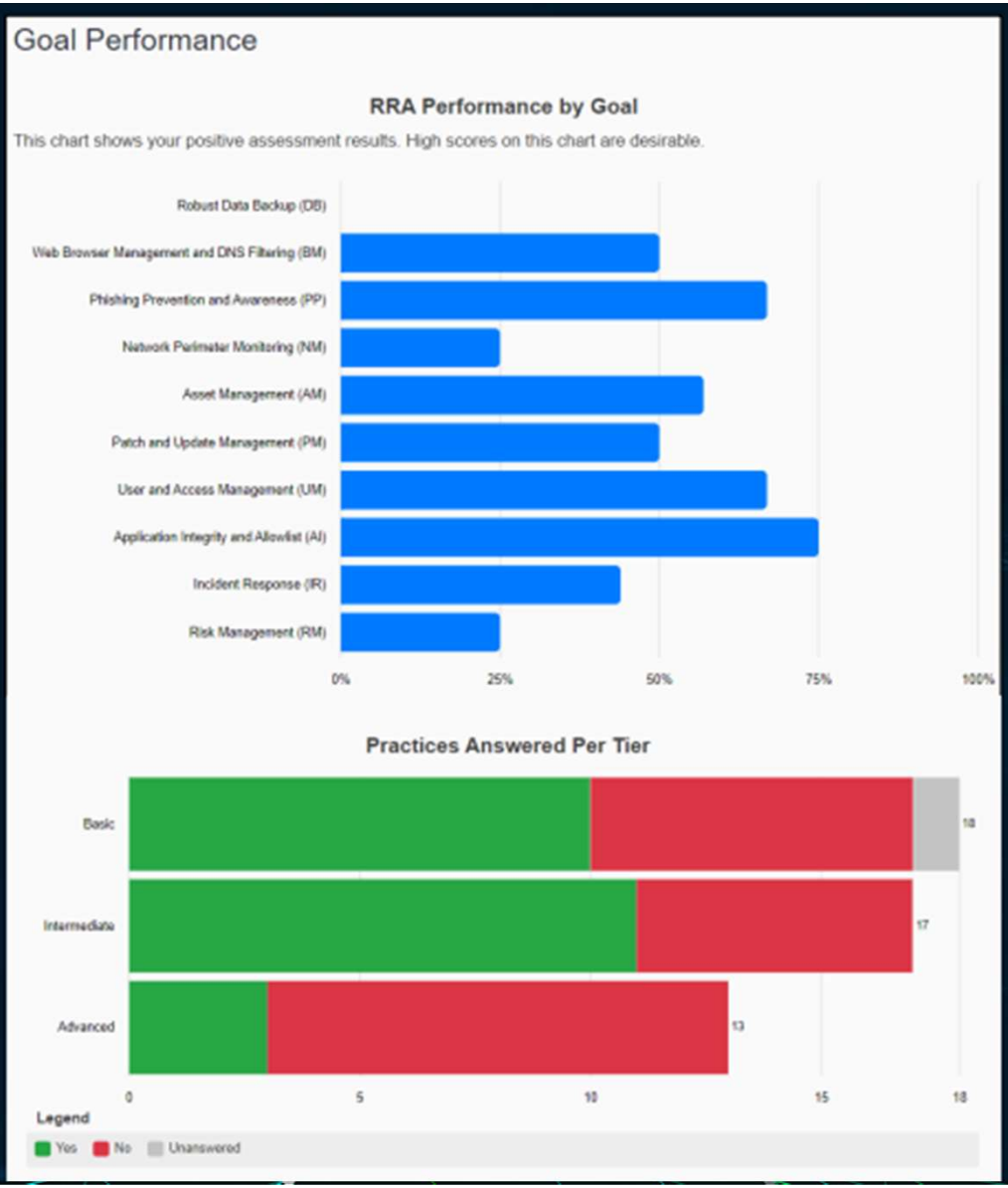


CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

POWERED BY CYBER FLORIDA at USF

Reports

Ransomware Readiness Assessment (RRA) (48 Questions)



Risk Assessment Overview

- Why
  - Assess and improve your cybersecurity posture by identifying risks, vulnerabilities, and areas for improvement.
  - Align with Florida's cybersecurity policies and regulations (e.g., F.S. 282.318).
- Who
  - Critical Infrastructure (CI) – Organizations that provide essential services such as energy, water, healthcare, finance, and transportation.
  - Private Sector – Businesses that work with or for CIs.
- When
  - Conducted annually to keep cybersecurity strategies up to date and adapt to evolving threats.
- How
  - Step 1: Organizations register through Cyber Florida's website.
  - Step 2: Complete the risk assessment questionnaire, aligned with NIST CSF 2.0 categories.
  - Step 3: Receive a customized risk report with insights on vulnerabilities and improvement recommendations.
  - Step 4: Access free tools, training, and resources to strengthen cybersecurity resilience.

Benefits

✅ Identifies cybersecurity gaps and vulnerabilities before they are exploited.

✅ Aligns with the latest NIST Cybersecurity Framework (CSF) 2.0 for structured risk management.

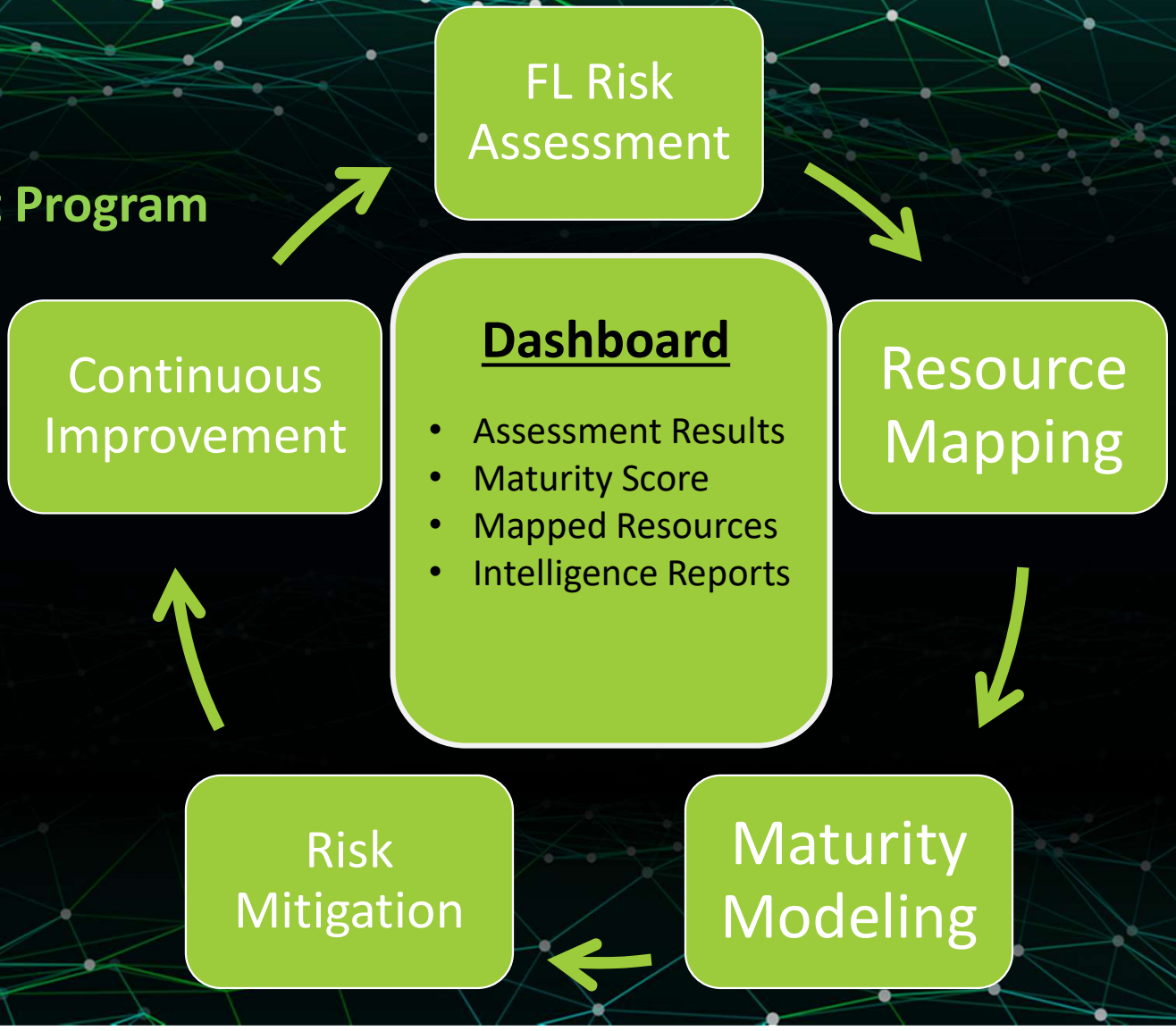
✅ Provides actionable insights and recommendations to improve security posture.

✅ Supports compliance with state and federal cybersecurity regulations.

✅ Enhances incident response capabilities by identifying weaknesses in preparedness.

✅ No-cost assessment available through Cyber Florida, reducing financial barriers.

Cyber Florida Cybersecurity Enhancement Program



Florida's "Whole of State" Cybersecurity

"Cohesive defensive framework for the entire state"

- F.A.C. 60GG-2: Florida Cybersecurity Standards (FCS)
  - Modeled after NIST CSF 1.1.
- F.S. 282.318: State Cybersecurity Act
  - Lead by Florida Digital Services (FLDS)
    - Establish asset management
    - Use a standard risk assessment methodology
    - Complete comprehensive risk assessment
    - Identify information protection procedures
      - Establish CIA procedures
    - Establish threat detection processes
    - IRP w/tiered reporting timeframes
    - Develop strategic and operational cybersecurity plans

Florida's "Whole of State" Cybersecurity

"Cohesive defensive framework for the entire state"

- **F.S. 282.319 – Florida Cybersecurity Advisory Council:**
  - This section establishes the Florida Cybersecurity Advisory Council
- **F.S. Chapter 501.171 – Data Security Breach Notification:**
  - This statute requires entities to take reasonable measures to protect personal information and mandates notification to affected individuals and the Department of Legal Affairs in the event of a data breach.

Florida Legislation:
Statutes 282.318, 282.3185, 282.3186

- Florida State Cybersecurity Act, Local Government Cybersecurity Act, and Ransomware Incident Compliance
- Identifies levels of severity of the cybersecurity incident (based on national standards)
- Identifies Florida Digital Service as the state lead
- Requires State Cybersecurity Operations Center (CSOC)
- Victims **may not pay or otherwise comply with** a ransom demand
- Identifies reporting requirements
  - Identifies required content of report
  - When to report
    - No later than **48 hours** after discovery of the cybersecurity incident
    - No later than **12 hours** after discovery of the ransomware incident
  - Who to report to:
    - State Cybersecurity Operations Center
    - Cybercrime Office of the Department of Law Enforcement
    - Local Sheriff

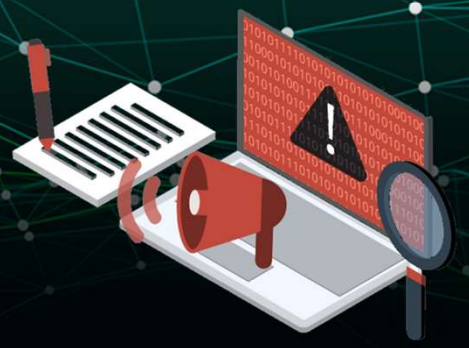
Level of Severity of the Cybersecurity Incident

- **Level 1** is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence
- **Level 2** is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.
- **Level 3** is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.
- **Level 4** is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties.
- **Level 5** is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the countries', states', or local government's residents.

Must be reported!

As defined by the National Cyber Incident Response Plan of the United States Department of Homeland Security

Reporting Requirements Details



The report must contain the following information:

- A summary of the facts surrounding the cybersecurity incident or ransomware incident
- The date on which the state agency most recently backed up its data; the physical location of the backup, if the backup was affected and if the backup was created using cloud computing
- The types of data compromised by the cybersecurity incident or ransomware incident
- The estimated fiscal impact of the cybersecurity incident or ransomware incident
- In the case of a ransomware incident, the details of the ransom demanded

On Behalf of Cyber Florida…