Florida Association of Counties Technical Workshop

Cyber Florida and FIU

January 30, 2025

Agenda

9:00am-9:05am	Welcome
9:05am-9:25am	Florida Risk and Intelligence update
9:25am-9:45am	Resources available to State Leaders, Community Partners and Sectors
9:45am – 10:05am	Federal and State Guidelines
5 min	Break (optional)
10:10am-10:30am	Scenario based discussion
10:30am-10:50am	Audience discussion (Q and A Session)
10:50am	Cyber Hygiene; here are the 5 things everyone needs to do

Why are we here? What are our outcomes today?

- You are not alone in understanding and addressing technology and cybersecurity as an organizational challenge and risk
- Cybersecurity means a lot of things, what should it mean to me
- **Cyber FL and FIU serve as your community partners**

Cyber Florida and FIU Team

- Dr. Alex Crowther – FIU (presenter)
  - gcrowthe@fiu.edu
- Emeka Okammor – Cyber FL (presenter)
  - emekaokammor@cyberflorida.org
- Bryan Langley – Cyber FL
  - bjlangley@cyberflorida.org
- Juan-Carlos Gonzalez del Valle – FIU
  - gonzajua@fiu.edu
- Melissa Da Gama – FIU
  - mdagama@fiu.edu

Florida Risk and Intelligence update

Mr. Okammor
Dr. Crowther

FIU
Jack D. Gordon Institute for Public Policy

Major Threats

Individual: Smart phone

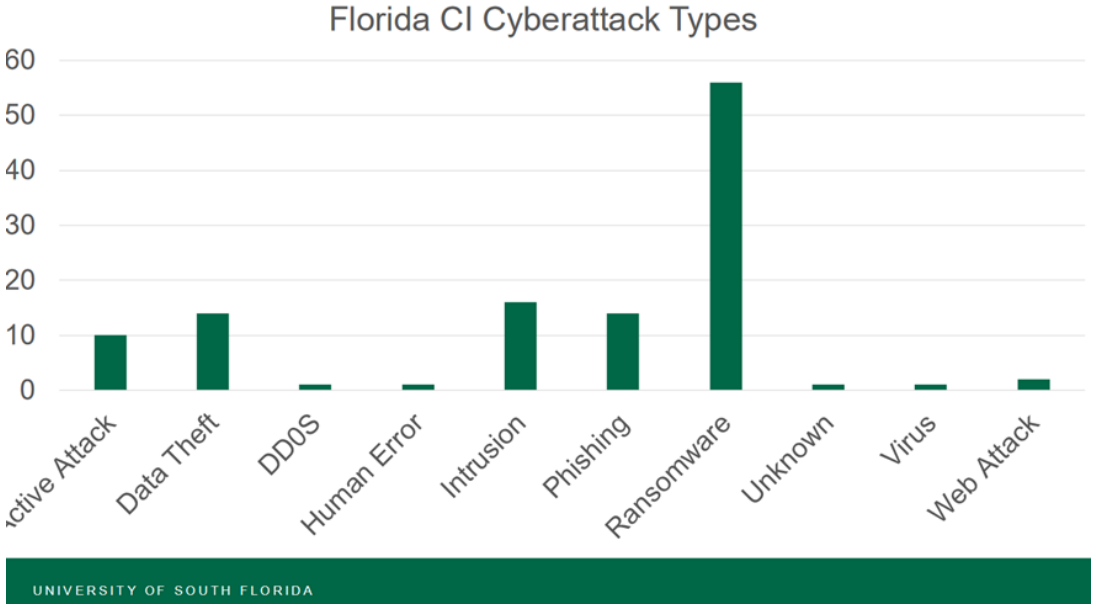
- End User Licensing Agreement (EULA)

Family: Internet of Things

- Lack of security allows access to router

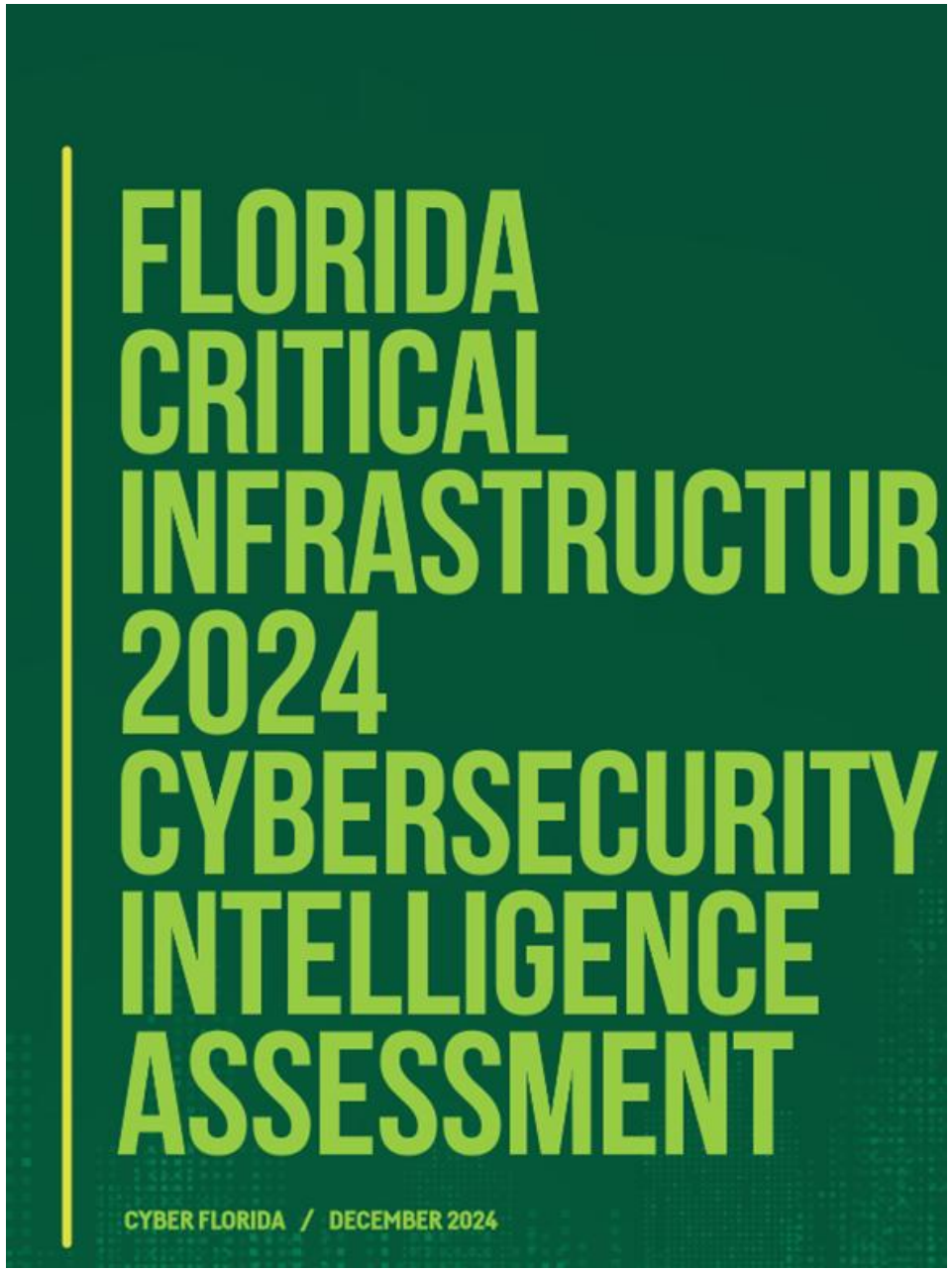
Organization: Insider Threat

- People are the weak point



CI Report: Key Takeaways

- Cyber ***threat*** level to CI (Florida and Na
  - Cyber Threat Actors (CTAs) are constantly access to CI systems
    - China, Russia, Iran, North Korea, Ransomware
- Primary cyber threats to CI sectors:
  1. Ransomware
  2. Data Theft
  3. Intrusion
  4. AI



Risks and Challenges Identified

The assessment revealed several significant gaps in Florida's CI sectors:

- 50% of CI providers lack response and recovery plans.
- 50% do not use Multi-Factor Authentication (MFA).
- 39% conduct response planning with third-party providers, but only 48% regularly audit these partners' cybersecurity practices.
- Nearly half (49%) lack formal cybersecurity training programs beyond basic awareness.
- Many providers do not have assigned cyber-management responsibilities, with 49% lacking a CISO.
- Less than half (48%) of organizations conduct biannual incident response tabletop exercises.
- Only 53% of CI providers have defined their risk tolerance, indicating a significant gap in risk management strategies.

Resources available to state leaders, community partners, and sectors

Cyber Florida Resources

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

FIU | Jack D. Gordon Institute for Public Policy

Cybersecurity Leadership and Strategy Professional Education Program

Take your cybersecurity training on the go!

Our state-funded cybersecurity training is now available virtually for public sector officials! Complete at your own pace in just two weeks!

Register online at

go.fiu.edu/CLSRegister

This state-funded cybersecurity training is only for eligible executive leadership, senior level management, public officials, and employees with access to highly sensitive data.

CYBER FLORIDA FIRSTLINE

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

This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

FIU | Jack D. Gordon Institute for Public Policy

Cybersecurity Leadership and Strategy Professional Education Program

CYBER FLORIDA FIRSTLINE

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

This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

You are Florida's first line of cyber defense.

Your leadership is key to making Florida cyber-ready. Our free training will help you build successful policies.

Contact Melissa Da Gama

mdagama@fiu.edu

to set up a group cybersecurity training on-site.

This state-funded cybersecurity training is only for eligible executive leadership, senior level management, public officials, and employees with access to highly sensitive data.

Cyber Florida Resources

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

Cyber Florida Resources

• 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

Cyber Florida Resources

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+

Cyber Florida Resources

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

Cyber Florida FCRA

Critical Infrastructure Protection (CIP) Program

- Free online cyber risk assessment funded by the State of Florida
- Entry-level assessment (20 questions) to identify vulnerabilities
- Mid-level assessment (38 questions) measuring against the Cybersecurity Performance Goals (CPG)s
- 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, etc.
- Close the maturity gap for “basic” ransomware readiness
- Mapping tool 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)

Federal and State Cybersecurity Guidelines

FIU
Jack D. Gordon Institute for Public Policy

Most Probable Cyber Operations

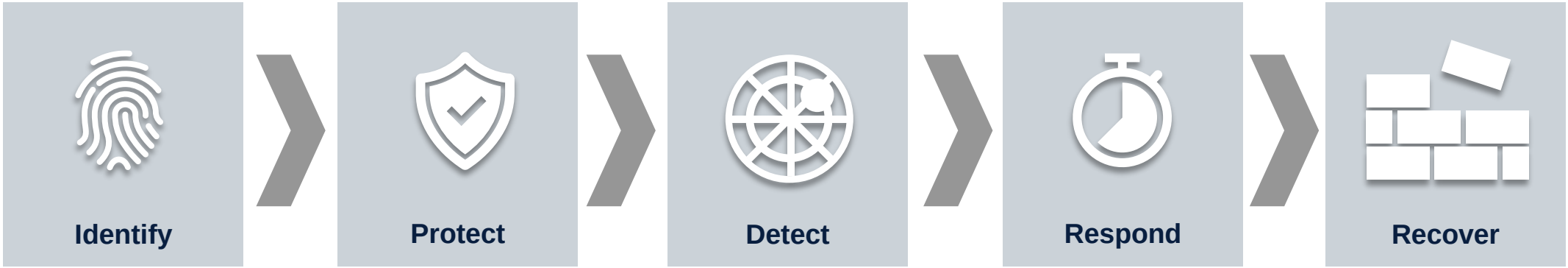
Actors	Targets: States	Intl Orgs	Proxies	Terrorists	Hacktivists	Business	Criminals	Populations	Co-Opted
States	Info	Info	Info	Info	Info	Info	Info	Info	Info
	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel
	Crime	Crime		Crime					
	Attack	Attack	Attack	Attack	Attack	Attack	Attack	Attack	Attack (through)
Proxies	Info	Info	Info	Info	Info	Info	Info	Info	Info
	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel
	Crime	Crime	Crime	Crime	Crime	Crime		Crime	Crime
	Attack	Attack	Attack	Attack	Attack	Attack	Attack	Attack	Attack
Terrorists	Info	Info	Info	Info	Info	Info	Info	Info	Info
	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel
	Crime	Crime		Crime		Crime	Crime	Crime	Crime
	Attack	Attack	Attack	Attack	Attack	Attack	Attack	Attack	Attack
Hacktivists	Info	Info	Info	Info	Info	Info	N/A	Info	Info
	Intel	Intel	Intel	Intel	Intel	Intel			Intel
		Crime							
	Attack	Attack	Attack	Attack	Attack	Attack			Attack
Business	Info	N/A	Info					Info	N/A
	Intel		Intel	Intel	Intel	Intel	Intel	Intel	
						Crime			
				Attack?			Attack?		
Criminals	Info	Info	Info	Info	Info	Info	Info	Info	Info
	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel
	Crime	Crime	Crime	Crime	Crime	Crime	Crime	Crime	Crime
							Attack		
Populations	Info	N/A	N/A	N/A	N/A	N/A	Info	Info	N/A
	Intel						Intel	Intel	

CYBER FLORIDA FIRSTLINE
No-cost education & training for Florida's public sector
This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

FIU
Jack D. Gordon Institute for Public Policy

NIST Cybersecurity Framework

- **New with NIST 2.0: Governance - Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy**
- 5 Key Pillars – Holistic and successful program
- Highest level of abstraction – Minimum standards
- Lexicon for management to express their cybersecurity management



- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

- Identity Management, Authentication & Access Control
- Awareness & Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance
- Protective Technology

- Anomalies & Events
- Security Continuous Monitoring
- Detection Processes

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

- Recovery Planning
- Improvements
- Communications

Source: NIST Cybersecurity Framework

FIU
Jack D. Gordon Institute for Public Policy

Most Common Cyber Operations Techniques

Entry Operations

- Phishing
- Spear Phishing
- Whaling
- SMShing (SMS)
- Video Phishing
- Voice Phishing
- Quishing (QR Code)

Entry Operations, cont.

- Password Spraying
  Top 20 passwords:
  - password
  - 123456
  - 12345678
  - 1234
  - qwerty
  - 12345
  - dragon
  - (an inappropriate word for female genitalia)
  - baseball
  - football
  - letmein
  - monkey
  - 696969
  - abc123
  - mustang
  - michael
  - shadow
  - master
  - Jennifer
  - 111111

Injecting Malware

Money Making

- Includes ransomware

Obtaining Information

- Includes ransomware

CYBER FLORIDA FIRSTLINE
No-cost education & training for Florida's public sector
This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

FIU
Jack D. Gordon Institute for Public Policy

Cyberspace Operation Sequence

	Timing	Action
1	**Before Initial Entry**	Identify effect you desire Selection of target (Social Engineering) Prepare initial entry malware
2	**Initial Entry**	Phishing operation Placing software or hardware into the system
3	**Reconnaissance**	Exploring the network Identifying system administrators and leaders Assessing vulnerabilities
4	**Preparation to create effect**	Putting in backdoor Changing software to allow you to create an effect
5	**Creation of effect**	Moving money Opening dam sluice gate Denial of Service (DoS)

CYBER FLORIDA FIRSTLINE
No-cost education & training for Florida's public sector
This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

FIU
Jack D. Gordon Institute for Public Policy

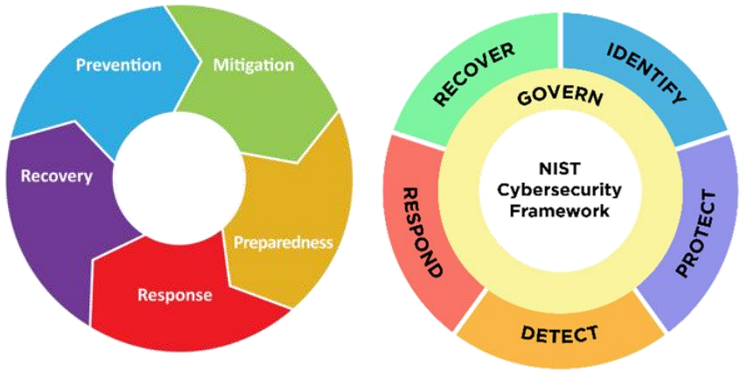
Cyberspace Defense Sequence

FEMA

NIST National Institute of Standards and Technology

FEMA	NIST		Good for
Prevent	**Identify**	Governance	Strategies and plans for the inevitable
Protect			Cyber hygiene to prevent 80-90%
Mitigate	**Detect**		Detect operation to catch the 10-20%
Respond			
Recover			

Governance:
"Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy"



[FEMA Mission Areas and Core Capabilities] & [NIST Cybersecurity Framework]

FIU
Jack D. Gordon Institute for Public Policy

Paying a Ransom In Florida

Florida Law 282.3186 Ransomware incident compliance.—A state agency as defined in s. 282.318(2), a county, or a municipality experiencing a ransomware incident **may not pay or otherwise comply** with a ransom demand.

CYBER FLORIDA FIRSTLINE
No-cost education & training for Florida's public sector
This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

FIU
Jack D. Gordon Institute for Public Policy

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

CYBER FLORIDA FIRSTLINE
No-cost education & training for Florida's public sector
This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

FIU
Jack D. Gordon Institute for Public Policy

Reporting Cyber Incidents In Florida

- Codified in the “State Cybersecurity Act, Local Government Cybersecurity Act, and Ransomware Incident Compliance”
- Report to:
  - Florida State Cybersecurity Operations Center
  - Cybercrime office at the Department of Law Enforcement (FC3)
- Florida Digital Service - Cybersecurity Operations Center
- FDLE/FC3:
  - FDLE Computer Crime Center: https://www.fdle.state.fl.us/FCCC
  - Report a Computer Crime: https://www.fdle.state.fl.us/FCCC/Report-a-Computer-Crime.aspx
  - FC3 Email address: FDLECyber@fdle.state.fl.us

FIU
Jack D. Gordon Institute for Public Policy

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.

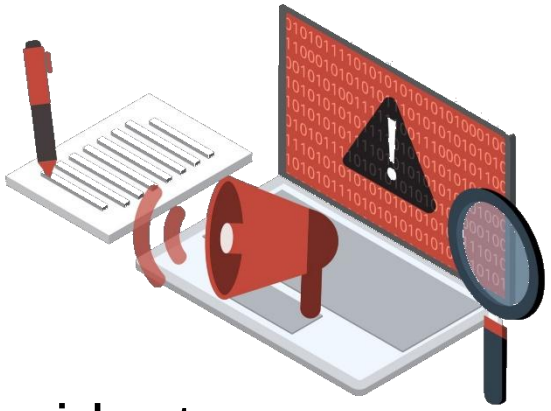
Must be reported!

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

CYBER FLORIDA FIRSTLINE
No-cost education & training for Florida's public sector
This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

FIU
Jack D. Gordon Institute for Public Policy

Reporting Requirements Details

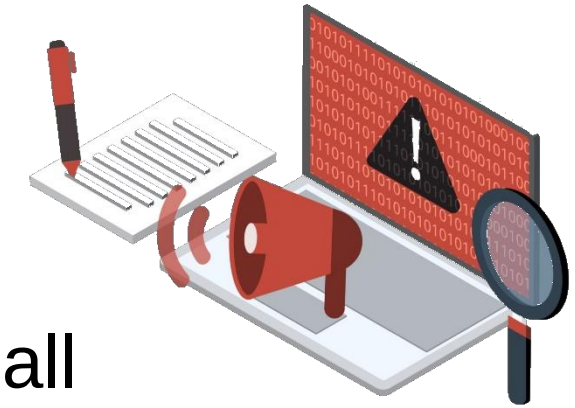


The report must contain the following information:

- 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

FIU
Jack D. Gordon Institute for Public Policy

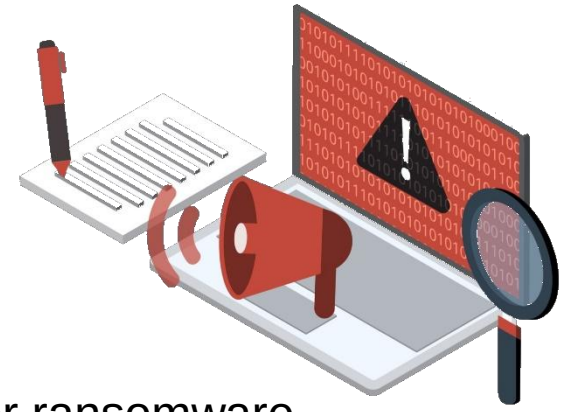
Reporting Requirements Florida



A state agency or local government shall report all ransomware incidents and any cybersecurity incident determined by the state agency to be of severity level 3, 4, or 5 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible but **no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident** (i.e. when you receive a ransom demand)

FIU
Jack D. Gordon Institute for Public Policy

Reporting Requirements Local Government



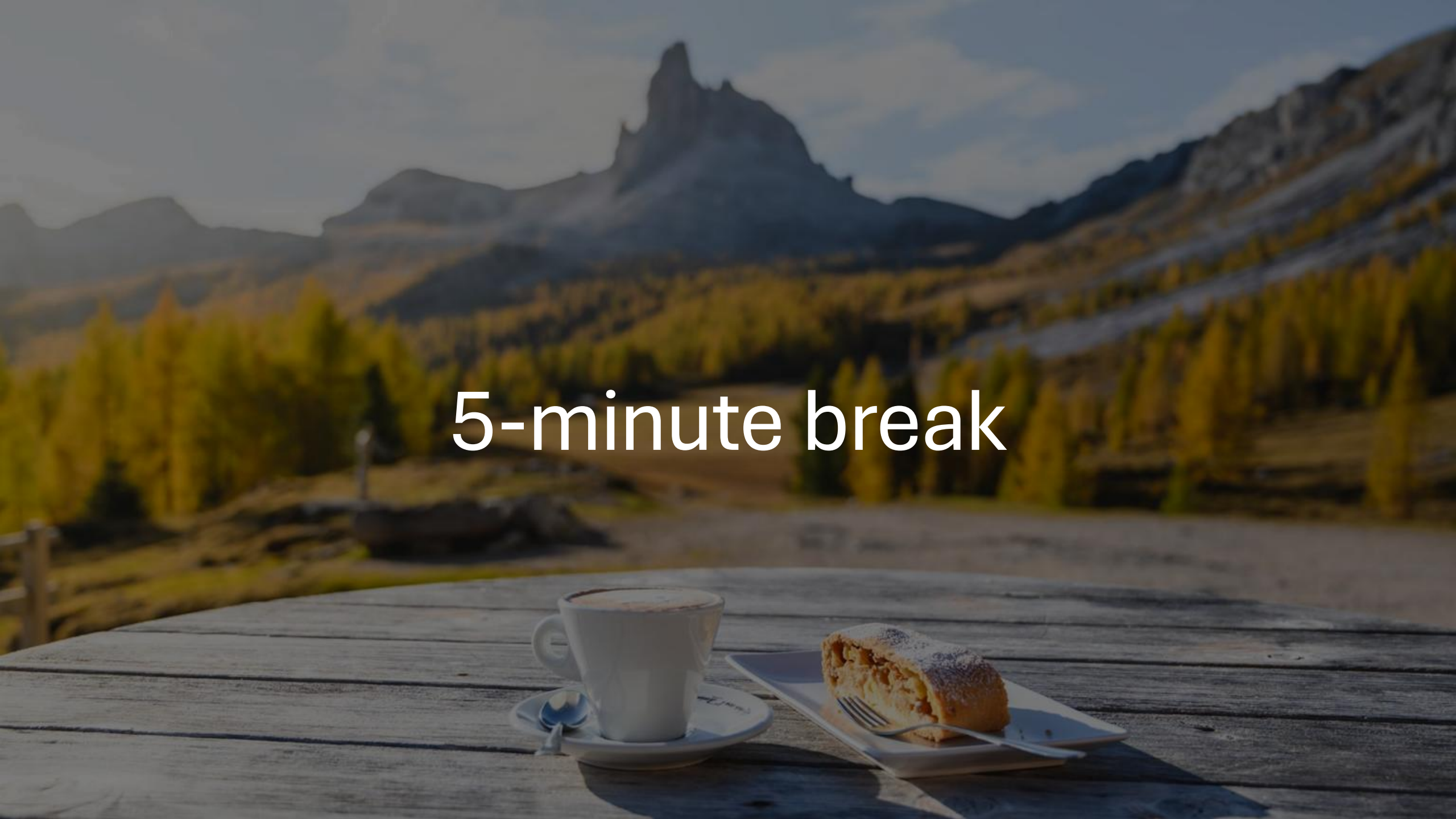
In addition to the previous reporting requirements,

- A local government shall provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of the Department of Law Enforcement, **and Sheriff who has jurisdiction over the local government**

They also must add the following:

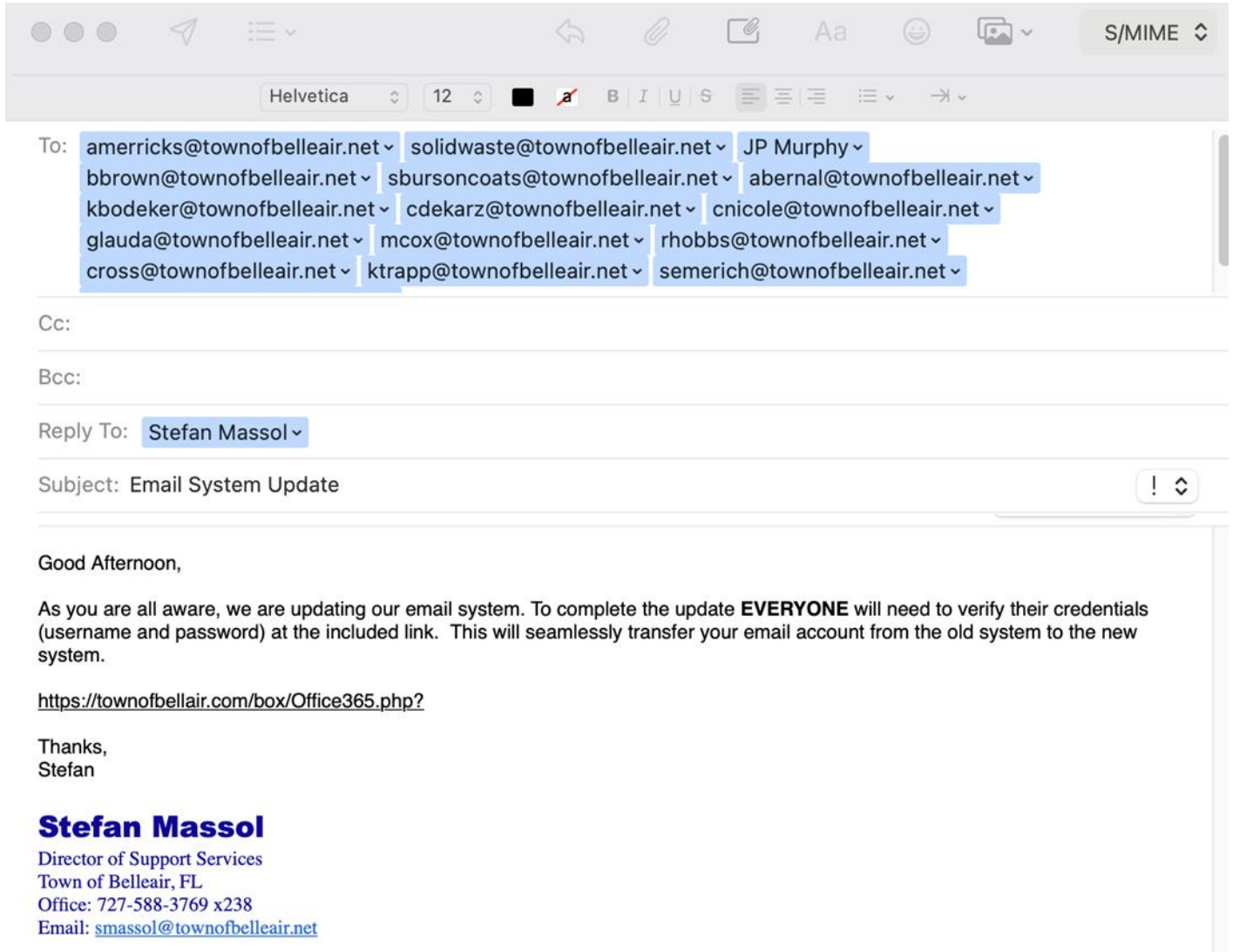
- A **statement requesting or declining assistance** from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government
- A local government must submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, **an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident**.

CYBER FLORIDA FIRSTLINE
No-cost education & training for Florida's public sector
This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.


5-minute break

Scenario based discussion

Step 1: Spear phishing e-mail



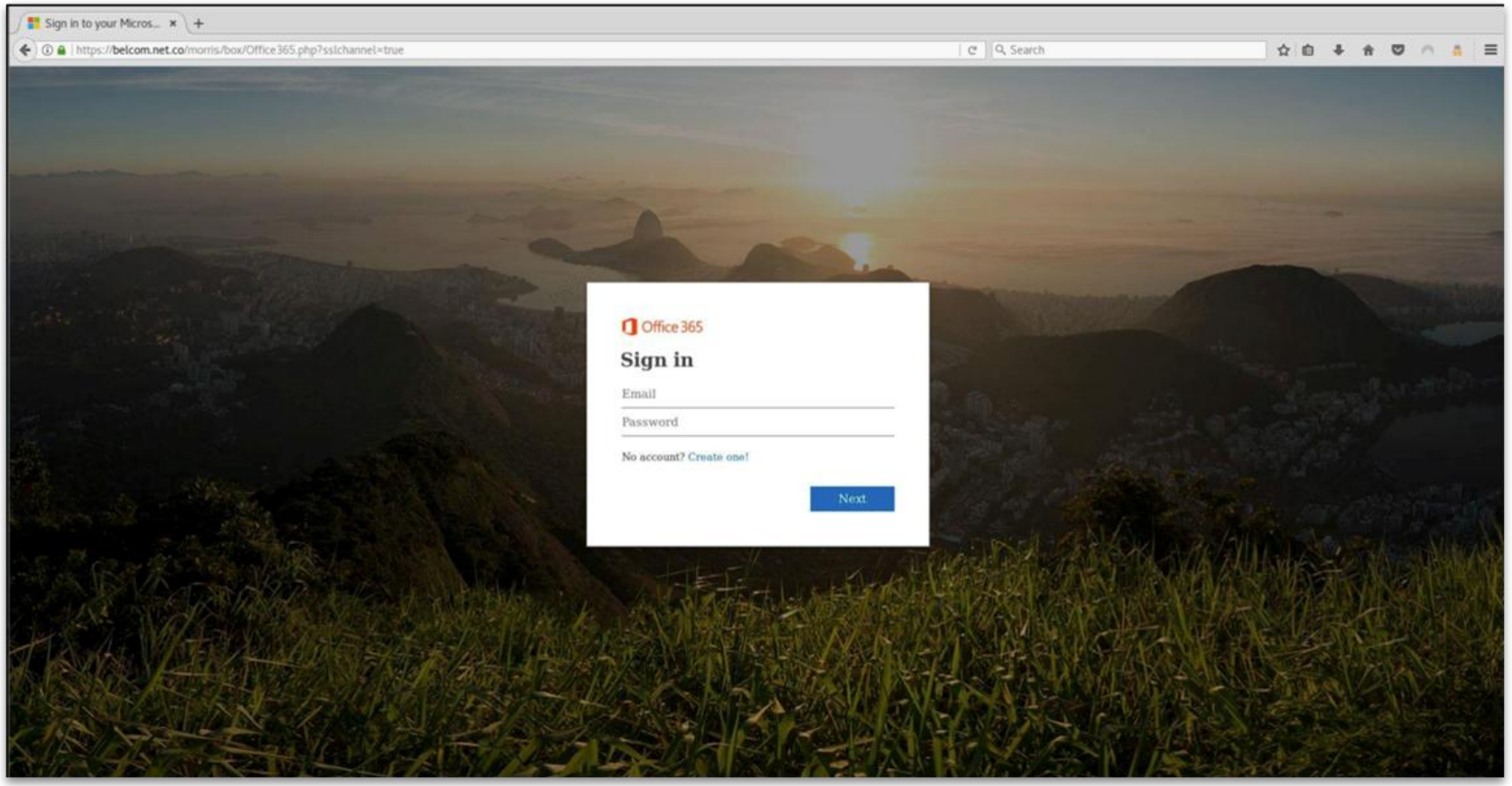
Phishing Stats

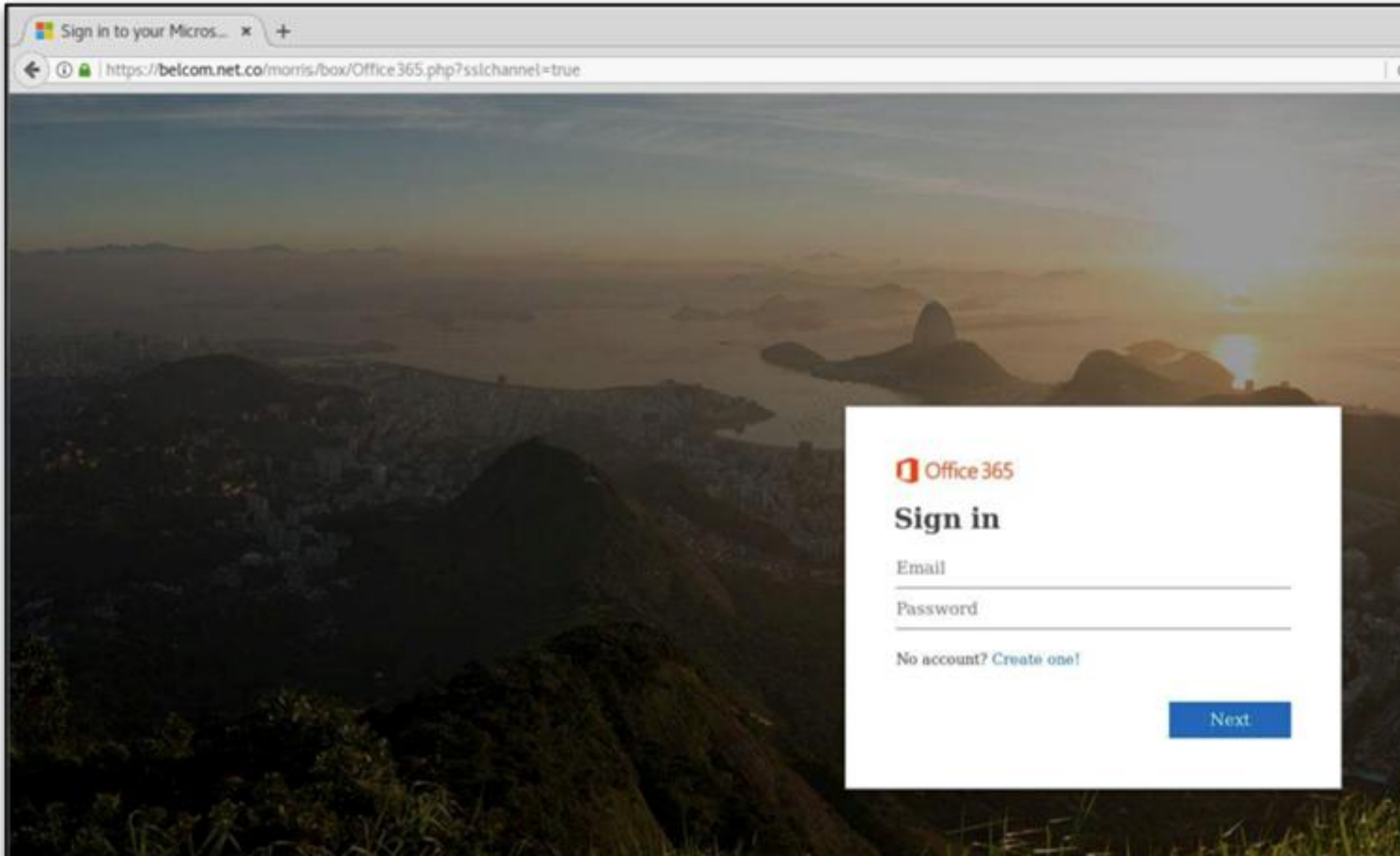
Attack Vector: Phishing is the number one attack vector, with 91% of cyber attacks starting with a phishing email

Global Reach: Spear phishing emails constitute less than 0.1% of all emails sent but are responsible for 66% of all breaches.

Financial Impact: In 2023, Florida reported 1,711 BEC incidents, resulting in losses totaling approximately $193.8 million.

Step 2: Credential Harvesting




Sign in to your Micros...
https://belcom.net.co/morris/box/Office365.php?sslchannel=true
Office 365
Sign in
Email
Password
No account? Create one!
Next

Credential Harvesting Stats

Attack Vector: Phishing is the number one attack vector, with 91% of cyber attacks starting with a phishing email

Global Reach: Spear phishing emails constitute less than 0.1% of all emails sent but are responsible for 66% of all breaches.

Financial Impact: In 2023, Florida reported 1,711 BEC incidents, resulting in losses totaling approximately $193.8 million.

9 in 10 Employees

This is how many employees are willing to engage in risky behaviors and do things that they know may put your business in jeopardy.

Discussion

- Does your organization have a formalized Cybersecurity Training Program?
  - What does the training cover?
  - Is training required to access the network?
  - How often are employees required to complete the training?
- What about third-party vendors with access to your network, do you require/offer training?
- Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?

Step 3: Impacted Network Performance

- Several employees call the IT help desk complaining about sluggish machines
- IT works to resolve the issue, most users are instructed to restart their machines
- Many users report temporary improvements after rebooting, but some continue to experience sluggish performance, with certain programs freezing or crashing.
- IT begins to escalate the issue for further analysis, suspecting it could be related to a system-wide update or a malfunctioning software update that rolled out recently.

Step 4: Ransom

- IT is working diligently to identify the root cause.
- Ransomware images appear on numerous users' computers, they also appear to be locked
- The message on the computer screens states, "all files are encrypted" and demands payment of 17 Bitcoins for the decryption key
  - 17 Bitcoins = 1,779,007.50
  - The message warns the key will expire in 48-hours

Ransomware

- Do you pay the ransom? **No**
  - FL HB 7022 states it is illegal to pay ransom
  - F.S. 282.318(2) states it is illegal for counties, cities, and state agencies to pay ransomware
- Do you have back ups?
  - Are they air gapped?
  - Are they immutable?
  - Have they been tested?
- Do you have cyber risk insurance?
  - Do you know or have access to your coverage details?
  - When do you put in a claim?
- What outside partners/entities do you need to contact?
  - Do you have a breach notification policy?

Step 5: Public Relations

- The Local news contacts your Agency's PIO and inquires about reports of a potential ransomware attack
- Additional media calls are received requesting comments on the ransomware incident.
- The media is not going away, there is increased interest on Social Media

PIO Discussion

- How would your agency respond to the news inquiries and the public's comments on social media?
  - Have pre-scripted messages have been developed for cyber incidents?
  - What training does your communications personnel receive on cyber terminology?
  - How would public messaging be coordinated and disseminated during a cyber incident impacting the agency?
  - How would your agency work to maintain the public's confidence and trust during these incidents?
  - What are your additional public affairs concerns?

Step 6: Post Ransom

- The deadline for the ransom payment has passed, the workstations are still locked
- Several employees advised they have not received their direct deposits for the current pay period, despite receiving notifications they were paid
- HR and Finance teams are investigating the issue and have contacted the bank to confirm payment processing status. A temporary manual payroll system is considered as a contingency.
- Meanwhile, the media continues to pressure the organization for updates on the ransomware attack, including how it is impacting day-to-day operations and employee compensation.

Key Takeaways

- **Cyber Threats Are Inevitable**
  - Attacks are no longer a question of “if” but “when.”
  - A single phishing email can lead to millions in losses and operational chaos.
- **Resilience Comes from Leadership & Strategy**
  - Cybersecurity is **not just an IT issue**—it’s an organizational issue.
  - Executives and policymakers must drive a **culture of cybersecurity** across all departments.
- **Proactive Planning Reduces Downtime & Damage**
  - Invest in **air-gapped, immutable backups** and test them regularly.
  - Ensure **crisis response teams** know their roles **before** an attack occurs.

Key Questions

- Does our agency have a **documented and tested** incident response plan?
- Do we **train all employees & vendors** on cyber risks and protocols?
- Are our backups **secure, tested, and quickly restorable** in a crisis?
- Have we engaged **cyber insurance and legal experts** to navigate financial impacts?

Final Thought: Cybersecurity is a shared responsibility. Every department, every employee, and every leader must play a role. The time to act is **before** an attack, not after.

Cyber Hygiene

FIU
Jack D. Gordon Institute for Public Policy

Cyber Hygiene

- Don’t click on the link!
  - Be aware of phishing
- Decent, unique passwords
- Multifactor Authentication (MFA)
- Keep software updated
- Antivirus
  - Set to scan before downloading
- Virtual Private Network (VPN)
  - Prevents others from seeing your traffic
  - Set to auto-engage whenever touching the internet
- Backup your data
  - Cloud; On-site, or a combination
- Create a continuity plan
  - What happens when you receive a ransomware operation?

CYBER FLORIDA FIRSTLINE
No-cost education & training for Florida's public sector
This program is provided at no cost to Florida public-sector employees through the Cyber Florida: FirstLine initiative funded by the Florida Legislature and led by Cyber Florida at USF.

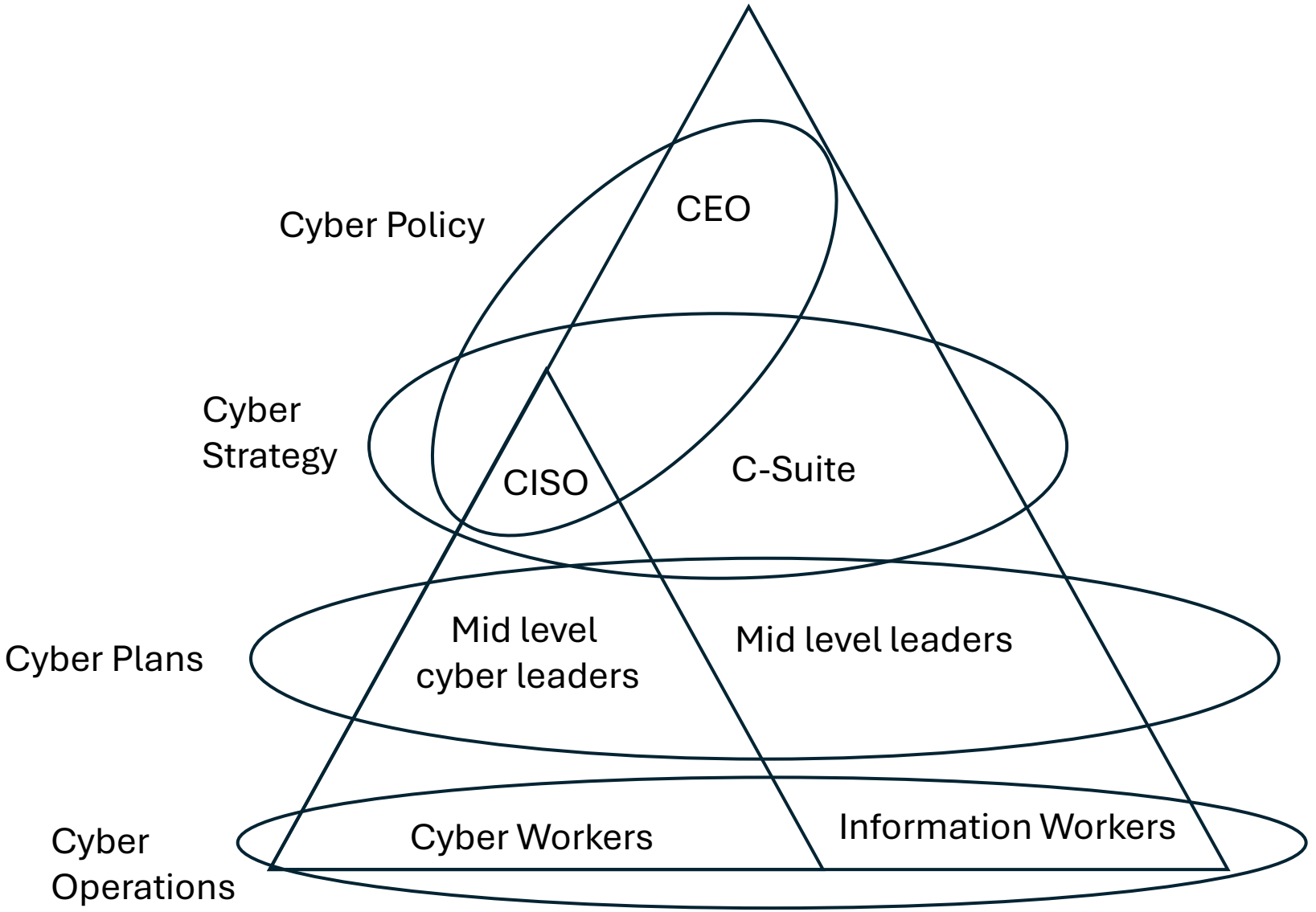
FIU
Jack D. Gordon Institute for Public Policy

FL Cybersecurity Advisory Council on Cyber Hygiene

- **Count** - Know what's connected to your network
- **Configure** - Implement key security settings to help protect your system
- **Control** - Limit and manage those who have administrative privileges to change, bypass, or override your security settings
- **Patch** - Regularly update all applications, software, and operating systems
- **Repeat** - Regularize to form a solid foundation of cyber security for your organization

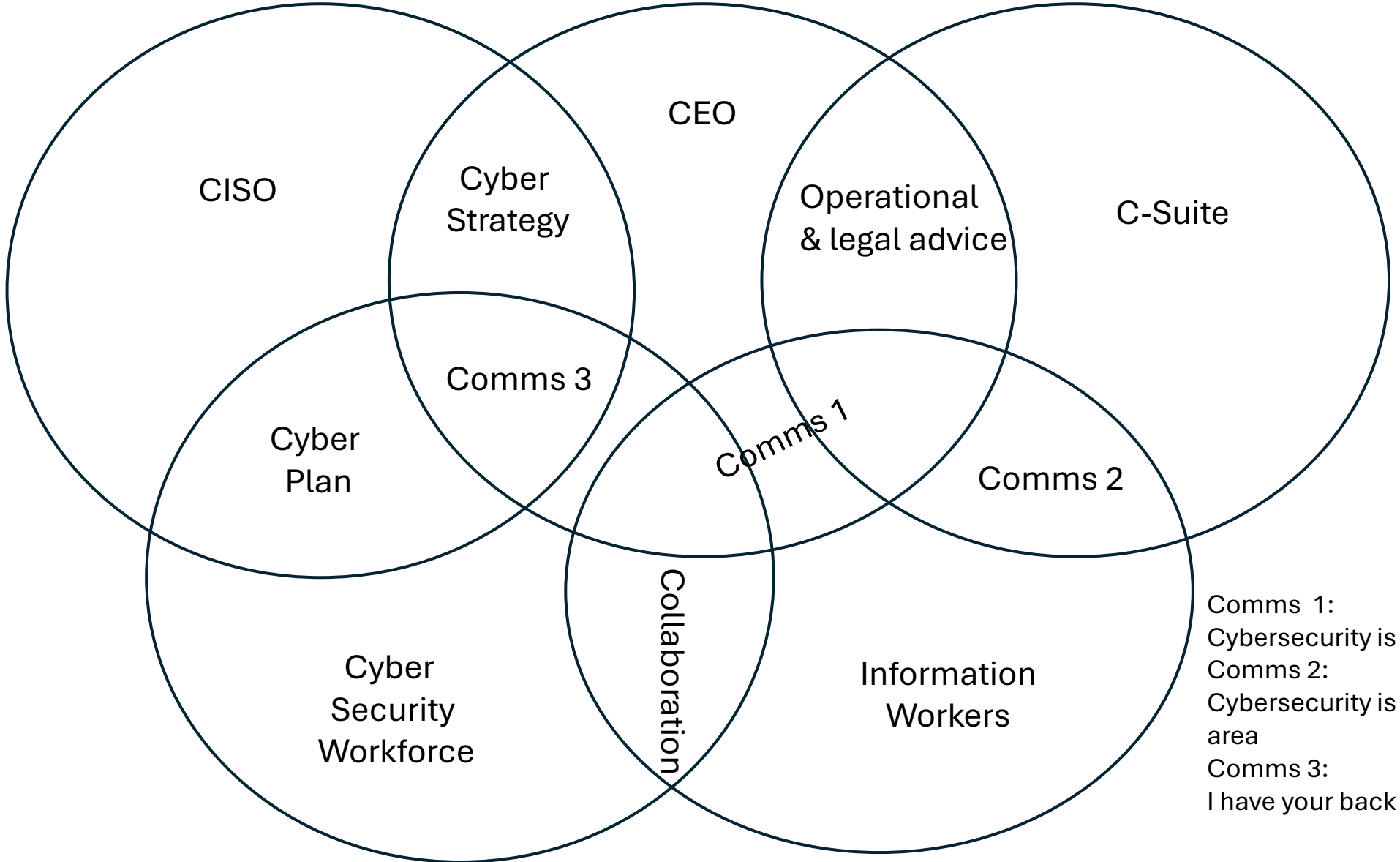
Source: https://www.dms.myflorida.com/other_programs/cybersecurity_advisory_council/cybersecurity_resources

How it should be...



Information Worker = anyone who uses a computer or smartphone

Communications within an organization



Comms 1:
Cybersecurity is important
Comms 2:
Cybersecurity is important in our area
Comms 3:
I have your back

Questions