

Cyber Florida: **FIRSTLINE**

Cyber Security Leadership & Strategy Course Sign In



URL: <https://wkf.ms/3ZXACP8>
Updated 6/2026

We will begin shortly.

Registration QR

Cyber Florida: **FIRSTLINE**

Cyber Security Leadership & Strategy Course Sign In



URL: <https://wkf.ms/3sBBw7E>

Updated 6/2026

We will begin shortly.

Sign In QR

Cyber Florida: FIRSTLINE

Cyber Security Leadership & Strategy Course Sign In



We will begin shortly.

Cybersecurity and AI for Government Finance Officers

Florida Government Finance Officers
Association

Mike Asencio

October 27, 2026





Jack D. Gordon
Institute for Public Policy

Reporting Requirements

**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 - Internal / Private

Florida Legislation: Statutes 282.318, 282.3185, 282.3186

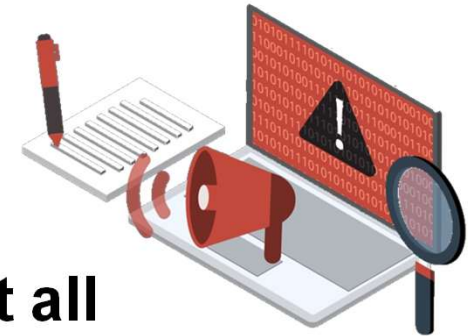
- Florida State Cybersecurity Act, Local Government Cybersecurity Act, and Ransomware Incident Compliance
- Identifies levels of severity of the cybersecurity incident (based on national standards)
- Identifies Florida Digital Service as the state lead
- Requires State Cybersecurity Operations Center (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

(S)

(P)



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)

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!

(T)

(S)

(P)

(O)

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

FIU - Internal / Private

	General Definition	Observed Actions	Intended Consequence ¹
Level 5 <i>Emergency</i> (Black)	<i>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.</i>	Effect	Cause physical consequence
Level 4 <i>Severe</i> (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</i>	Presence	Damage computer and networking hardware
Level 3 <i>High</i> (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Presence	Corrupt or destroy data Deny availability to a key system or service
Level 2 <i>Medium</i> (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Engagement	Steal sensitive information
Level 1 <i>Low</i> (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Engagement	Commit a financial crime
Level 0 <i>Baseline</i> (White)	Unsubstantiated or inconsequential event.	Preparation	Nuisance DoS or defacement

Figure 2: Cyber Incident Severity Schema

<https://www.cisa.gov/sites/default/files/2024-12/NCIRP%20Update%20Public%20Comment%20Draft%20508c.pdf>

FIU - Internal / Private

Reporting Requirements Local Government



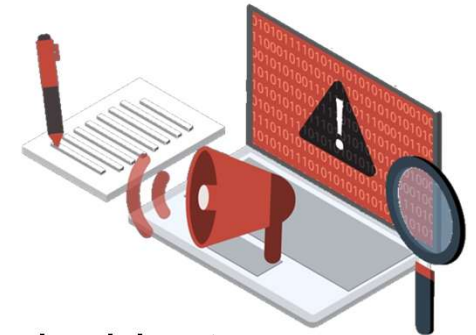
In addition to the previous reporting requirements,

- 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.**

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

(P)

(O)

Report an Incident

Florida Digital Service Cybersecurity Operations Center

- Email: CSOC@digital.fl.gov
- Phone: 850-631-1334, 850-412-6074
- Web https://ir.digital.fl.gov/ir_form.html

When reporting an incident you may request assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction (for local governments only).

<https://ir.digital.fl.gov/>

After Action Report

- In addition, state and local governments are required to provide an after-action report within one week of remediation.
- To satisfy this post-incident reporting requirement, an after-action form is available for download. Completed forms must be submitted to CSOC@digital.fl.gov.
- Download:
<https://ir.digital.fl.gov/download/FLDS-CSOC-After-Action-Report-Form.docx>



Florida Digital

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



The Reality

- 🚨 Cyberattacks are **increasing in frequency**, scale, and sophistication
- 💰 **Financial impact is accelerating faster** than overall incident volume
 - *Losses ↑ ~5× since 2020 IC3 DATA*
- ⚙️ Most organizations struggle to operationalize enterprise cybersecurity
- 🚒 Investment in incident response is reactive, often after a major event
- 👤 Qualified **cyber talent shortages** continue to widen
- 🔗 **Third-party risk adds complexity** across legal, compliance, and security domains
- 🤖 **Automated, AI-driven attacks**

(S)

Cybersecurity strategy will help shift from a **reactive** approach to a **proactive** posture.

FIU

Jack D. Gordon
Institute for Public Policy

Emerging Threats & Cybersecurity Strategy

**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 - Internal / Private



Role of Leaders in Cybersecurity

Senior Leaders

Decide. Fund. Communicate. Oversee.

- Define what matters most to the organization
- Set policies & priorities
- Approve strategy (Ends, Ways, Means)
- Allocate resources
- Communicate importance of cybersecurity
- Build a security-minded culture
- Oversee performance & reporting

CIO/CISO

Interpret. Recommend. Execute. Report.

- Interpret laws & policies
- Recommend policies & frameworks
- Translate leadership goals into technical strategy
- Manage resources & execution
- Keep leadership informed

 **Takeaway:** Cybersecurity failure is rarely technical it's usually governance.



City of Atlanta's Cyberattack

- In **March 2018**, hackers targeted Atlanta's computer networks.
- Demanding **\$51K** in bitcoins, the cyberattack held the city hostage for nearly a week.
- Some city **services reverted to pen and paper** to continue operations.
- The **city refused to pay**: It didn't want to reward and encourage more ransomware attacks, and there was no guarantee that systems would be restored even if it paid.
- Ultimately, the financial hit to the city was far higher than the ransom.
- Costs associated with the attack reached **\$12M+**
- The episode marked an important moment of truth for the city.
- **Atlanta was unprepared** for such a major disruption, but it was clear that hackers had targeted cities before and would continue to do so for the foreseeable future.
- Atlanta's response wasn't just about recovering from a single incident: It was also about building a foundation for responding to future attacks.



(S)

(P)

(O)

Lessons Learned From the City of Atlanta's Cyberattack

- **Lack of cybersecurity strategy** for detecting, preventing and recovering from ransomware attacks
- Lack of **vulnerability patch management**
- No periodic and consistent **testing of systems' backups**
- **Not a formal incident response plan**
- **Lack of documented** disaster recovery (DRP) and business continuity plans (BCP)
- **Security gap assessments** and **risk analysis** not performed consistently
- **Cybersecurity underfunded**



People: No IR ownership, underfunded
Process: No patching, no DR testing
Technology: Vulnerability gaps

“City of Atlanta officials highlighted the importance of protecting government data and information, and of bringing discipline to an agency's approach to cybersecurity.”

FIU

Jack D. Gordon
Institute for Public Policy

CYBER SECURITY BUDGET BEFORE A BREACH



CYBER SECURITY BUDGET AFTER A BREACH

CYBERSECURITY EXPECTATION



CYBERSECURITY BUDGET

**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.

Cyberspace Operations Effects

(T)

Cyberspace actions that create various direct denial effects in cyberspace and manipulation leading to denial that is hidden or manifested in physical domains

- (a) **Manipulate.** To control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives
- (b) **Deny.** To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents adversary use of resources
 - 1. **Degrade.** To deny access to, or operation of, a target to a level represented as a percentage of capacity
 - 2. **Disrupt.** To completely but temporarily deny access to, or operation of, a target for a period of time
 - 3. **Destroy.** To permanently, completely, and irreparably deny access to, or operation of, a target

(O)

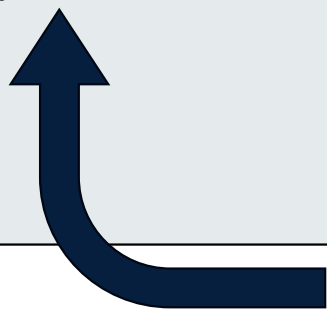
Source: Department of Defense Joint Publication 3-12 page II-7

FIU - Internal / Private

Types of Cyber Operations

(T)

Event	Description	
Cyber Operations	Any action taken in cyberspace	
Information Operation	Cognition shaping, much of which happens in cyberspace	May include ransomware
Intelligence Operation	Gathering important information and analyzing it; much information gathering happens in cyberspace	Includes most ransomware
Cyber crime	Crime that occurs in cyberspace. Important and growing number of cyber operations	May include ransomware
Cyber attack	An armed attack in cyberspace. Usually requires one of these results: <ul style="list-style-type: none"> • Property damaged • Property destroyed • Person hurt • Person killed 	Requires attribution!



Usually not a threat for State, Local, Tribal & Territorial (SLTT)

FIU - Internal / Private

Cyberspace Operation Sequence

(T)

	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)

Cyberspace Defense Sequence



FEMA

NIST

National Institute of
Standards and Technology

FEMA	NIST	Good for
Prevent	Identify	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

Governance:

“Establish and monitor the organization’s cybersecurity risk management strategy, expectations, and policy”



Source: [FEMA Mission Areas and Core Capabilities](#) & [NIST Cybersecurity Framework](#)

FIU - Internal / Private

NIST frameworks: cyber and AI

Topic	NIST CSF 2.0	NIST AI RMF 1.0
Focus	Cybersecurity risks to systems and services	AI risks to people, organizations and society
Core functions	Govern, Identify, Protect Detect, Respond, Recover	Govern, Map Measure, Manage
Governance	Govern guides the other functions	Govern spans Map, Measure and Manage
Finance example	Protect payment access and restore finance systems	Check AI drafts for errors and control data use

CSF and AI RMF support complementary risk decisions.
AI RMF 1.0 is voluntary. NIST is revising it.

Sources: [NIST CSF 2.0](#), [NIST AI RMF 1.0](#)



NIST AI RMF for finance officers

Function	Finance office application
Govern	Set permitted uses, data rules and responsibility for review
Map	Identify the task, affected people and potential consequences
Measure	Test calculations and sources. Track errors and unsupported claims
Manage	Require human approval. Monitor results and pause use when needed



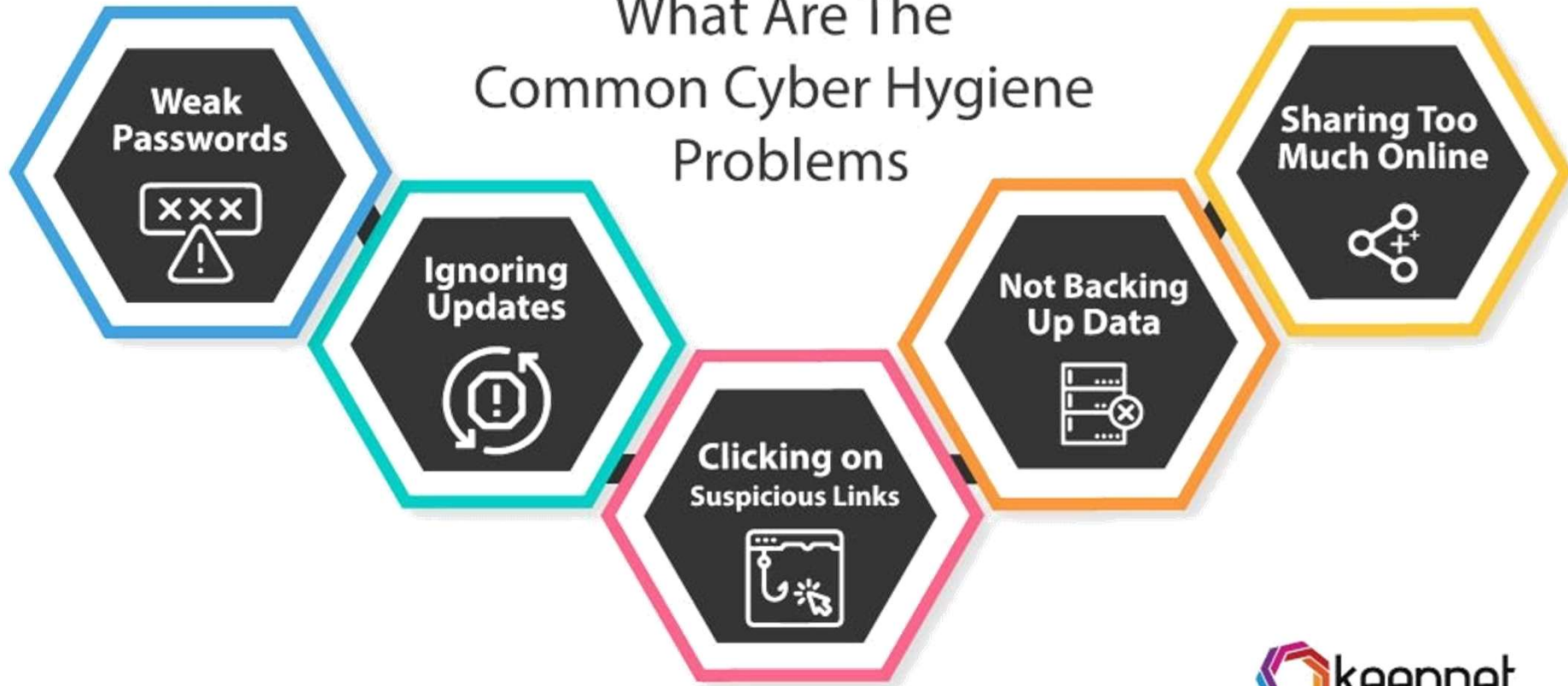
Govern applies across Map, Measure, and Manage.

Sources: [NIST CSF 2.0](#), [NIST AI RMF 1.0](#)

The Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Devices	Asst Mgmt. Vuln Scanning	EPP/EDR/Patch Mgmt.	EDR, EUBA, XDR	EPP Response	Restore from Image
Application	Inventory of Apps (Cloud/OnPrem)	WAF, CASB	CASB		Restore Backup
Networks	Netflow, Vuln Scanner	FW/IDS/IPS	IDS	DDoS Response NW Forensics	
Data	Data Classification	Data Encryption/DLP	Deep/Dark Web FBI, DHS		Restore Backup
Users	Phishing Simulation	Security Awareness	Insider Threat/Behavior Analytics UBEA	User Lockout/Disable	Clean User account,
Degree of Dependency	<div> <div>Technology</div> <div>Process/Governance</div> </div>				
					People

What Are The Common Cyber Hygiene Problems



Most Common Cyber Operations Techniques

Entry Operations

- Phishing
- Spear Phishing
- Whaling
- SMSing
- Video Phishing
- Voice Phishing



Entry Operations, cont.

- Password Spraying

Top 20 passwords:

- | | |
|--|------------|
| • password | • letmein |
| • 123456 | • monkey |
| • 12345678 | • 696969 |
| • 1234 | • abc123 |
| • qwerty | • mustang |
| • 12345 | • michael |
| • dragon | • shadow |
| • (an inappropriate word for female genitalia) | • master |
| • baseball | • Jennifer |
| • football | • 111111 |

Injecting Malware

Money Making

- Includes ransomware

Obtaining Information

- Includes ransomware



 Scam Type	 What It Looks Like
 Toll/DMV Texts	“Unpaid tolls” or “DMV suspension” with a link
 Gov’t Impersonation Calls	Caller claims to be FTC/IRS “agent,” pushes Bitcoin ATM or gift cards
 AI Voice “Family Emergency”	A cloned voice of a loved one asks for urgent money
 Fake Job / Reshipping	“Remote role” to repackage goods or onboarding via chat apps
 Romance + Crypto (“Pig-Butchering”)	New online “partner” guides you to a crypto site with fake profits
 Crypto ATM Cash-Out	Scammer keeps you on phone, directs cash into Bitcoin ATM
 Holiday Crypto Promos	“Christmas bonus: deposit \$1k, get \$3k credit”
 Deepfake Medical Ads	Celeb/doctor “endorses” miracle cream/device
 AI Phishing & BEC	Polished emails, QR codes, supply chain look-alikes
 Negative-Option Billing	“Free trial” → recurring charges you didn’t consent to

Sunday 3:38 PM

Florida Sunpass, our records indicate that your vehicle has an unpaid toll invoice. To avoid additional charges of \$75.90 please settle your balance of \$7.59 at

sunpasstollsbill.com



Delivered

Stop. Think.
Don't Click
That Link.



Breaking Down the Brad Pitt Scam: How it Happened and What We Can Learn



the imposter declared love for her and proposed marriage, so Anne divorced her husband, who gave her a settlement of €775,000.

An estimated 12,000 people in France alone lost money in 2024 due to this kind of scam, highlighting the growing need for increased awareness and vigilance with online interactions.

<https://www.mcafee.com/blogs/internet-security/brad-pitt-romance-scam-explained-how-to-prevent-scams/>

FIU - Internal / Private

There's issue with your American Express account



American Express <administraciones@pentagon-seguridad.cl>

To hashedout@thesslstore.com

Reply

Reply All

Forward



Fri 11/8/2019 5:29 AM



This message was sent with High importance.

If there are problems with how this message is displayed, click here to view it in a web browser.



Review Your Information.

Due to recent activities on your account, we placed a temporary suspension until you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

[Click here to review your account now](#)

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,

American Express Company. All rights reserved

FIU

Jack D. Gordon
Institute for Public Policy



Mon 12/6/2021 8:13 AM

[Redacted]

AUDIO <

>

PO/8970087430/AUDIO

To



This message was sent with High importance.



VM273834- [Redacted] .mp3.html
911 bytes

Message from [Redacted] server.

M-i-cr-o-so-ft a-c-c-ou--n-t
Li-st-en to y-o-ur vo-ice ca-ll

Rec-ipi-ent ID: [Redacted]

Dat-e: 2021-12-06

Du-ra-tion: 02:23

Do-wn-lo-ad A-t-t-ac-h-m-e-n-t to l-i-ste-n

T-h-e m-es-sa-ge will be au-toma-tica-lly de-let-ed a-f-t-er 24 h-ou-rs

© 2021 Cor-por-at-ion

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

**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.

Sign in to your account

login.mcrsftsvm-app.digital/common/oauth2/v2.0/authorize?client_id=4765445...32c6-49b0-83e6-1d9376...

 Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

[Back](#) [Next](#)

 Sign-in options

[Terms of use](#) [Privacy & cookies](#)

Document Shared With You
milosh-solibella-0dcio.sgttommy.workers.dev

Sign in to your account
login.microsoftonline.com/common/oauth2/deviceauth

Microsoft

Enter code to allow access

Once you enter the code displayed on your app or device,

Do not enter codes from sources you don't trust.

F678S9PN9

Next

Terms of use Privacy & cookies

MZ
Milosh Zezelj
milosh@solibella.ch
Shared today at 11:22 AM · Requested your review

Revised_Statement_20260326.pdf

PDF · 1.1 MB Expires in 24 h

Review Requested

Milosh Zezelj: "Hi, please review and advice on the revised statement. Thanks!"

YOUR VERIFICATION CODE

F678S9PN9

Copy Code

Code valid for 14:44

How to access your document

1
Copy the code above

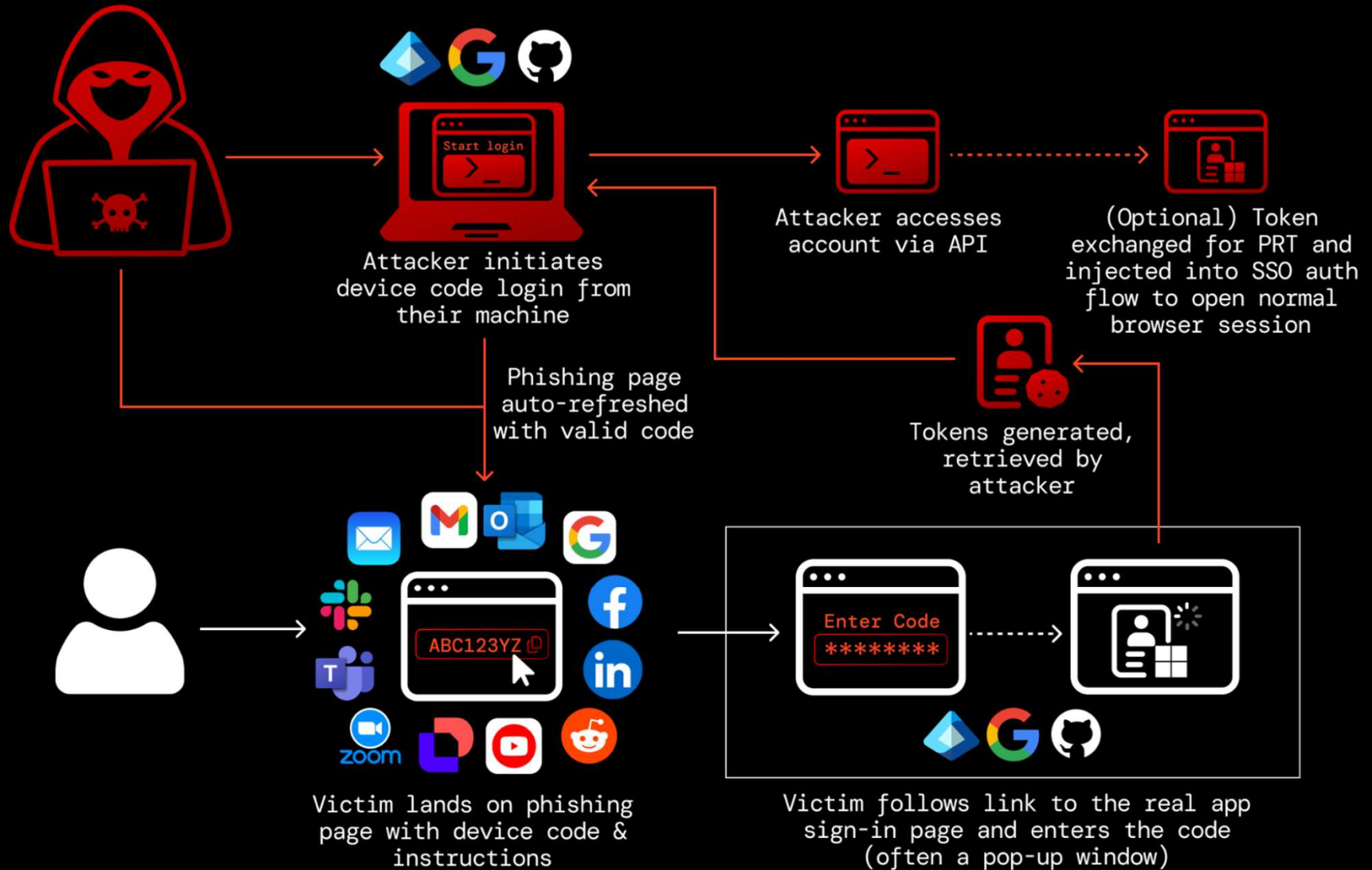
2
Click **Open Document** and paste when prompted (Ctrl+V)

3
Sign in with your Microsoft account to view

Open Document with Microsoft

Secured with end-to-end encryption · Adobe Document Cloud

Session 11889



Most Probable Cyber Operations

(T)

		Targets								
		States	Intl Orgs	Proxies	Terrorists	Hacktivists	Business	Criminals	Populations	Co-Opted
Actors	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		

FIU - Internal / Private

Most Probable Cyber Operations Against You

		Targets: State, Local, Tribal, Territorial			
Actors	States	Info	Intel	Crime	Attack
	Proxies	Info	Intel	Crime	Attack
	Terrorists	Info	Intel	Crime	Attack
	Hacktivists	Info	Intel		Attack
	Business	Info	Intel		
	Criminals	Info	Intel	Crime	
	Populations	Info	Intel		

(T)

(S)

(P)

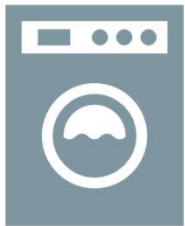
(O)

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



Terms of Service
Didn't Read

<https://tosdr.org>



<https://2fa.directory>

Insider Threats



MALICIOUS INSIDERS



**SOCIAL ENGINEERING
ATTACKS**



**INADEQUATE
MONITORING**



NEGLIGENT EMPLOYEES



THIRD-PARTY RISKS

Authentication

Less Bad: Password and...	Better: Password and...	Best: Passwordless
 SMS	 Authenticator app (push notifications)	 Authenticator app (passwordless)
 Voice	 Software Tokens OTP	 External security key
	 Hardware Tokens OTP	 Windows Hello
		 Passkeys

Authentication

MFA can block over 99.9 percent of account compromise attacks.

99%

Up to 73 percent of passwords are duplicates, this has been a successful strategy for many attackers and it's easy to do.

73%

FIU

Jack D. Gordon
Institute for Public Policy

**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.



What is Artificial Intelligence?

Machine Learning

Using sample data to train computer programs to recognize patterns based on algorithms.



Neural Networks

Computer systems designed to imitate the neurons in a brain.



Natural Language Processing

The ability to understand speech, as well as understand and analyze documents.

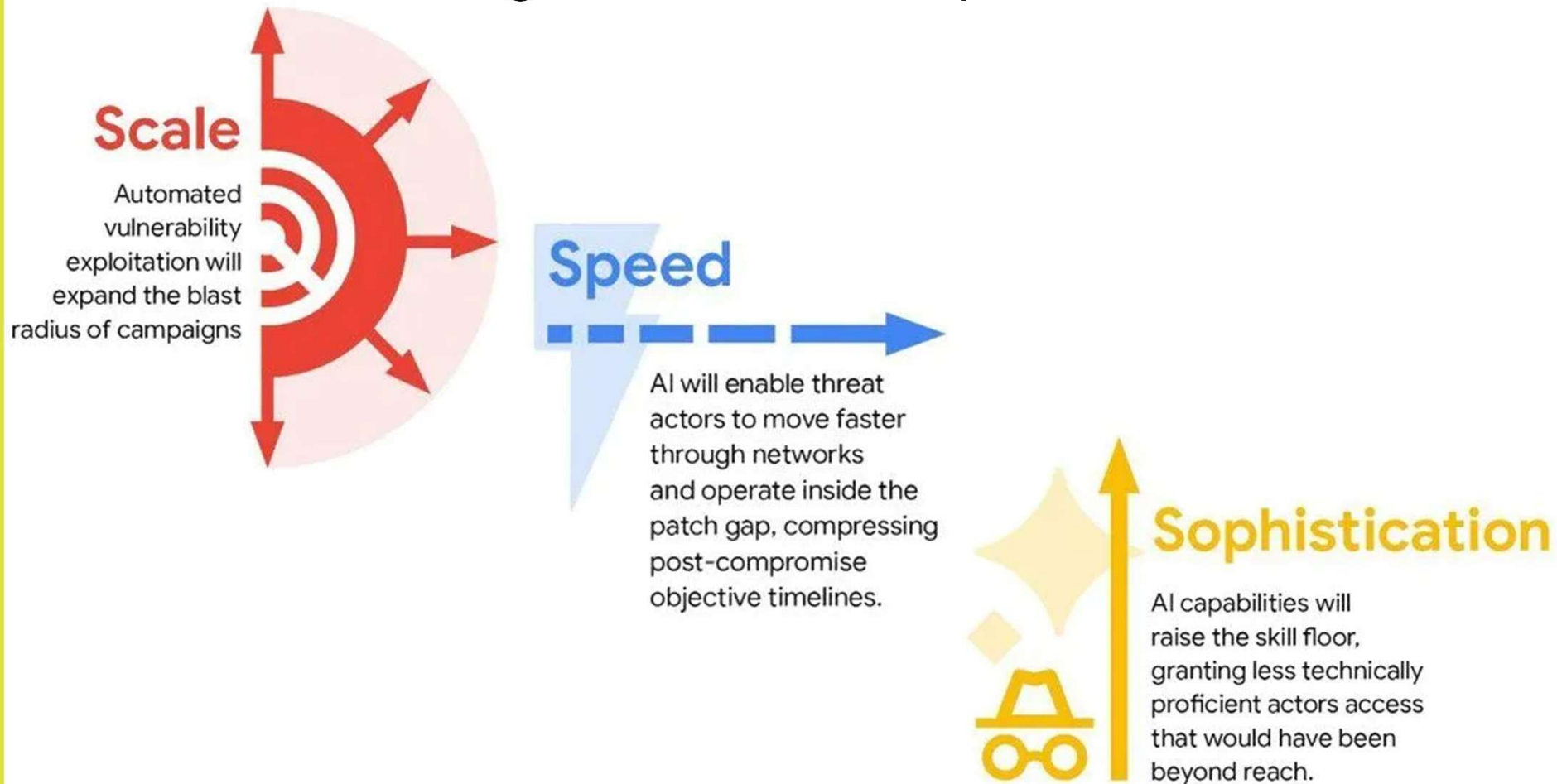


Robotics

Machines that can assist people without actual human involvement.



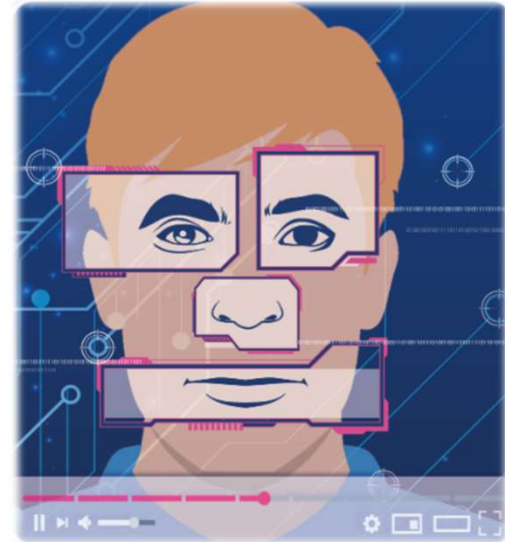
AI and the Evolving Threat Landscape



Case Study: Deepfake CEO Fraud — European Energy Firm (2024)

Attack Overview:

- Attackers used AI-generated voice deepfakes to impersonate the CEO in a phone call to the CFO
- The CFO authorized a fraudulent wire transfer (~\$243,000) believing he was following executive orders
- Multiple AI-synthesized follow-up calls sustained the deception and prevented verification



Impact & Implications:

- Financial: ~\$243,000 transferred; total recovery and legal costs far exceeded the original loss
- Operational: Emergency IR response, significant business disruption
- Industry-wide: Demonstrated that AI voice cloning is production-ready for fraud
- Regulatory: Sparked calls for mandatory multi-factor verification on all financial directives

Six Cybersecurity Risk Domains Introduced by AI

1. Data Privacy & Exposure

- AI systems ingest vast data; sensitive info may be leaked or misused during training

2. Model Manipulation

- Adversarial inputs can fool AI models into misclassifying threats or approving bad actions

3. Automated Threat Scaling

- Attackers automate phishing, scanning, and exploitation at speed impossible without AI

4. Social Engineering Enhancements

- Deepfakes and AI-generated text make BEC, vishing, and spear phishing far more convincing

5. Third-Party & Vendor Risks

- AI tools from vendors introduce new supply chain vulnerabilities and shadow AI exposure

6. Governance & Compliance

- Lack of AI policy frameworks creates regulatory exposure and ethical accountability gaps

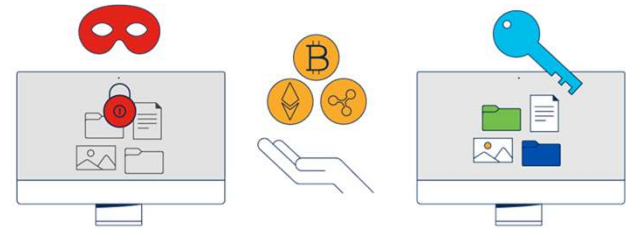
Florida Stat. 282.3185 governance requirements now explicitly apply to AI-related risks

Ransomware



What is Ransomware

- Ransomware is 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. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.
- Ransomware on the Dark Web
- New trends
 - Ransomware as a Service (RaaS)
 - Ransomware with data extortion and posting to dark web.



Why a focus on State & Local?

Source: <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware>

FIU - Internal / Private

jackpotjunction.com

PUBLISHED

Cash in on big wins this tax season! Every hour from 5 - 9 pm, one lucky winner will snag \$1,040 in CASH or Free Play! Earn just 25 points, print your voucher at a kiosk, and drop it in the

Updated: 24 Apr, 2025, 11:09 UTC

61407

ende.bo

PUBLISHED

Greetings! Today we are posting here the new company, "Empresa Nacional de Electricidad". Company Description: The National Electricity Company (ENDE) is a corporation of the

Updated: 16 Apr, 2025, 16:09 UTC

79151

crystal-d.com

PUBLISHED

At Crystal D, we have been manufacturing corporate gifts, recognition awards and crystal promotional products for more than 20 years.

Updated: 08 Apr, 2025, 11:42 UTC

48533

essenzamovies.com.br

PUBLISHED

acimfunds.com

PUBLISHED

Managing capital on behalf of institutional investors, family offices, and high net worth individuals. We focus on niche commodities strategies with an emphasis on the energy

Updated: 23 Apr, 2025, 11:08 UTC

61055

aeamg.org.br

PUBLISHED

Greetings! Today we are posting here the new company, "AEA-MG". Company Description: AEA-MG (Association of Electricians and Employees of CEMIG and its Subsidiaries) was founded on 29

Updated: 16 Apr, 2025, 16:07 UTC

51125

asiapacificex.com

PUBLISHED

employee documents(CEO included), corporate emails, finance, HR and many more! In case you cant find readme file: have a look at OBS cloud share: obs://apex-om-fileshare or obs://apex-

Updated: 06 Apr, 2025, 20:20 UTC

49768

unila.edu.mx

PUBLISHED

tuttoperlufficio.eu

PUBLISHED

E' definito molto più di un registratore di cassa. Nettun@ 3000 Touch Olivetti effettivamente concede agli esercenti una serie di opportunità che altri prodotti. ugualmente moderni e

Updated: 21 Apr, 2025, 10:00 UTC

61295

visionproducts.llc

PUBLISHED

Sed ultricies, diam et lacinia dapibus, diam dui semper nisl, ut dignissim diam lacus nec purus. In vitae volutpat velit, vitae rutrum enim. Ut tincidunt facilisis urna. egest dictum enim tincidunt vel.

Updated: 12 Apr, 2025, 13:06 UTC

46705

graphiquedefrance.com

PUBLISHED

Shop our Lifestyle & Gift Boutique for Designer Stationery, Journals, Planners, Calendars, Holiday, Home Decor, Greeting Cards, Gifts & beyond! Fashion Your Life with Graphique!

Updated: 06 Apr, 2025, 12:43 UTC

49104

osscc.mx

PUBLISHED

aqhch.com.cn

PUBLISHED

Heng Chang Machinery Co., Ltd (HCH), founded in 1988, is a leading world-class professional manufacturer of complete production lines for disposable hygiene products.

Updated: 16 Apr, 2025, 20:42 UTC

63434

physiciansmedicalbilling.net

PUBLISHED

Greetings! Today we are posting here the new company, "Physician's Medical Billing Inc". Company Description: Physicians Medical Billing (PMB) is a full-service medical billing and

Updated: 08 Apr, 2025, 22:07 UTC

51701

grupotersa.com.mx

PUBLISHED

Greetings! Today we are posting here the new company, "Grupo TERSA". Company Description: Grupo TERSA was born from the dream of our Chairman and Founder Rodriago Valle Hernández

Updated: 06 Apr, 2025, 12:38 UTC

54020

bioclimaservice.it

PUBLISHED

FIU

Jack D. Gordon
Institute for Public Policy

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.



Log In

SORTING

CREATED AT ↓

NAME



PCDPACKAGING.COM

[COMPANY URL](#) | [OCT 16, 2025](#)
5 photos | 0 files | 0.00 KB

Learn More

Development of customized industrial packaging. Single-use racks, export packaging, packaging for power units, specialized packaging, packaging for sea containers. 1.The document is an official bank statement from PCD Packaging de México S. ...







+
2 more





ARPIS.COM

[COMPANY URL](#) | [OCT 16, 2025](#)
4 photos | 0 files | 512.00 GB

Learn More

For fifty years, Arpi's has maintained this traditional approach to providing the highest quality service to our Calgary customers in the heating and cooling industry.Arpi's Industries is proud to be recognized for its services and commitment ...







FIU

Jack D. Gordon
Institute for Public Policy

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.

Home Databases Upgrades Search Hidden Service Escrow Extras

Login Register

BreachForums

Mark all as read Today's posts

General Leaks Marketplace Cracking Tech Staff

Leaks



Games

Game Leaks are posted here. Code, Plugins, Leaked Videos or anything similar to that may be posted here.

480
THREADS

4,629
POSTS

FIFA ONLINE SOURCE CODE L...
4 hours ago
by [arigato43](#)



Databases

Database leaks are posted here.

Official Databases Removed Content

8,753
THREADS

74,135
POSTS

[OGNIGGERS] India Insura...
21 minutes ago
by [cve1999](#)



Stealer Logs

Forum where you can post Stealer logs.

Stealer Logs Removed Content

3,589
THREADS

15,189
POSTS

4150 STEALER LOGS ⚡ FROM ...
1 hour ago
by [NEW_DAISSCLOUD](#)



Other Leaks

Ransomware Leaks, Stealer logs, Scrapes, Leads or other kinds of data that isn't considered a leaked database.

Other Leaks Removed Content

3,948
THREADS

28,907
POSTS

FREE 152sets ID DL Passpo...
12 minutes ago
by [FGG99](#)



Database Discussion

Forum where you can discuss & request databases.

Database Discussion Removed Content

1,241
THREADS

5,359
POSTS

DB Request <https://www.tr...>
18 minutes ago
by [Dark5029860](#)



Cracked Accounts

Cracked accounts for various platforms are posted here.

5,846
THREADS

87,959
POSTS

950+ ROBLOX ACCOUNTS CRA
C...
5 minutes ago
by [chy](#)



Combolist

Combolist are posted here (Cracked lines from Databases).

Combolist Removed Content

13,779
THREADS

88,216
POSTS

85K Fresh "roblox" URL:LO...
12 minutes ago
by [nwq](#)



HackTheBox

This forum is reserved for leaking HackTheBox Flags, this is a online game that tests your hacking skills.

1,021
THREADS

13,311
POSTS

DarkCorp Hack the Box Sea...
3 minutes ago
by [samuelballsiu1](#)



FBI's Internet Crime Complaint Center (IC3)

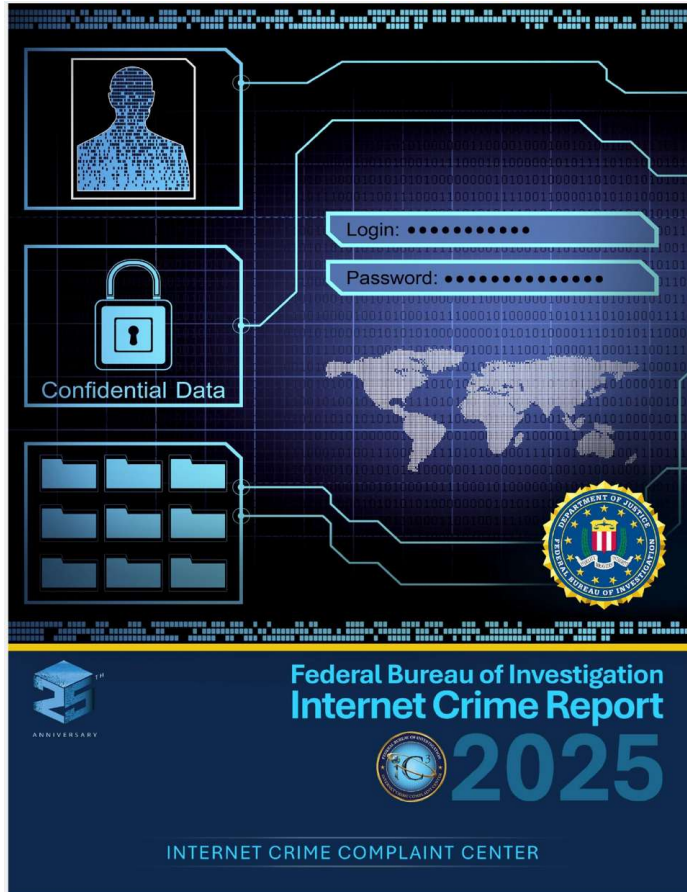
ic3.gov

IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include cyber threats and cyber-enabled fraud in their many forms including ransomware, intrusions (hacking), extortion, international money laundering, investment fraud, and a growing list of crimes.

IC3's mission is to provide the public and our partners with a reliable and convenient reporting mechanism to submit information concerning suspected cyber-enabled criminal activity and to develop effective alliances with law enforcement and industry partners to help those who report. Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and public awareness.

FIU - Internal / Private

2025 IC3 Report



1,008,597

Total complaints

\$20.877B

Total reported losses

+26%

Loss increase vs. 2024

\$20,699

Average reported loss

IC3 annual reports page

Lists the 2025 IC3 Annual Report plus companion state, younger, cryptocurrency, and elder-fraud reports.

ic3.gov/annualreport/reports

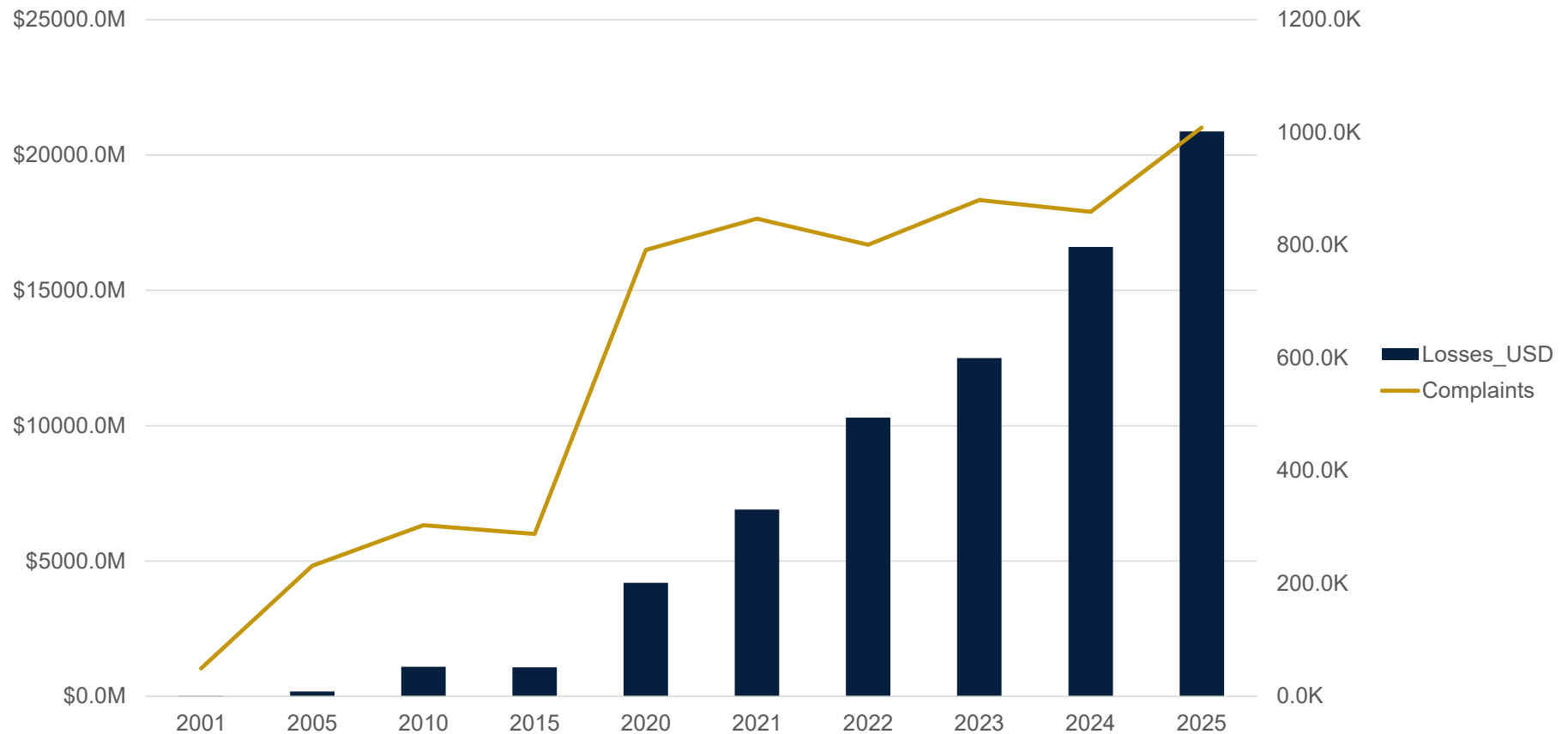
FBI press release

Summarizes the 2025 report and links back to the official IC3 report itself.

fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

2025 IC3 Report | Trends

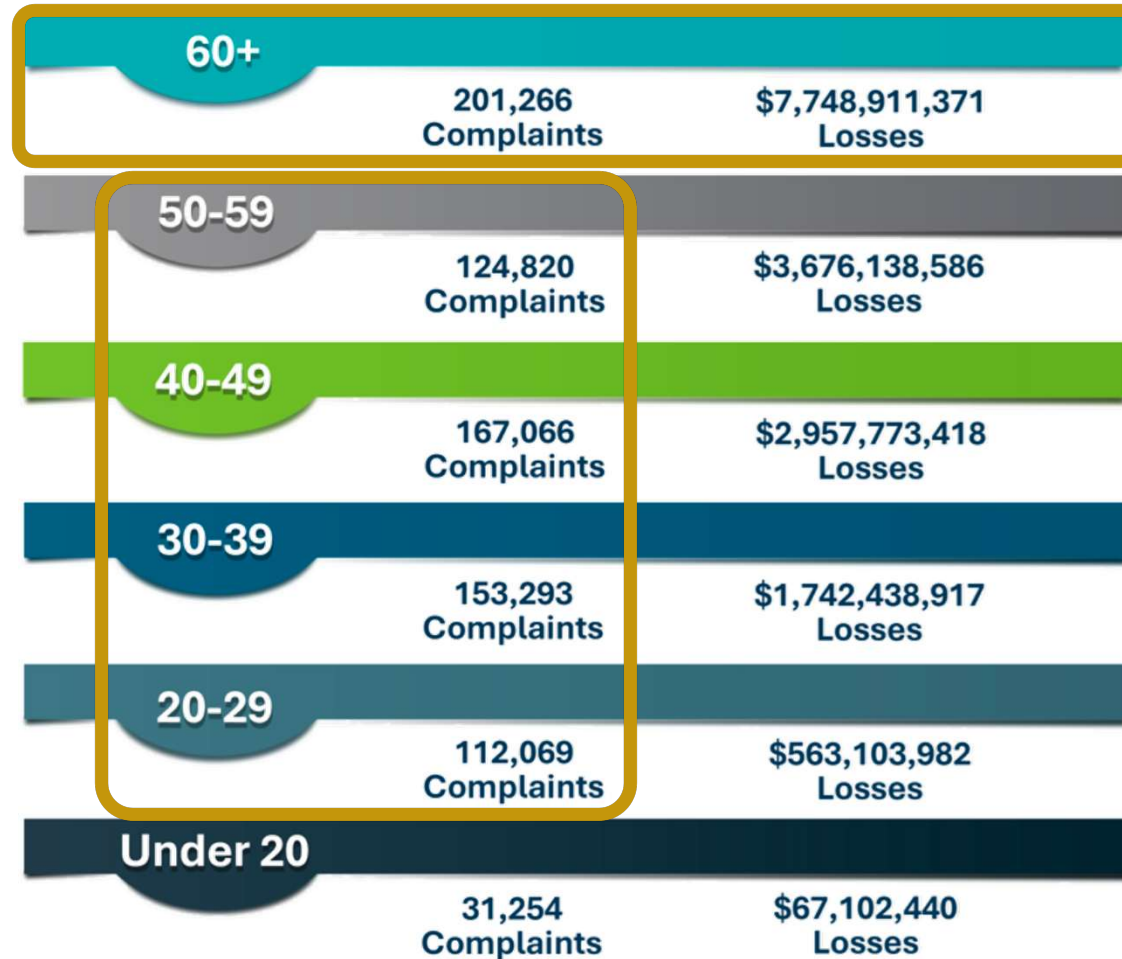
ICS3 Trends



FIU - Internal / Private

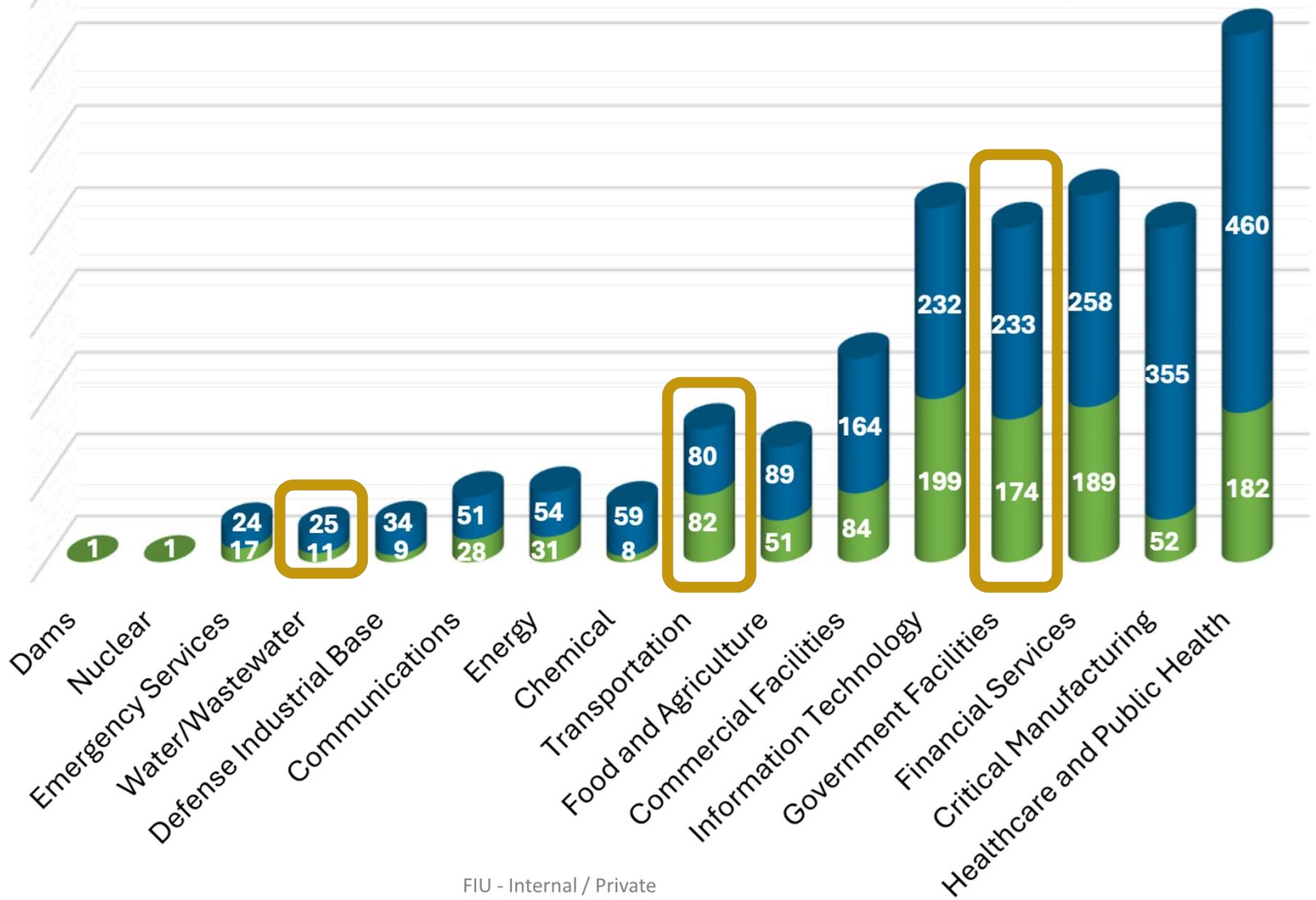
source: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

2025 COMPLAINTS BY AGE GROUP



Cyber Threats to Critical Infrastructure

■ Data Breach ■ Ransomware



FIU - Internal / Private

How is ransomware different from other cyber operations?

(T)

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

Create ransomware software

Execute ransomware operation

The Hidden Costs

Direct costs

- Incident response
- Legal fees
- Forensics
- Customer notification
- Credit monitoring

Operational costs

- System downtime
- Lost revenue
- Business disruption

Regulatory costs

- Fines
- Compliance penalties
- Lawsuits

Reputation costs

- Customer churn
- Stock impact
- Loss of trust

Florida Ransomware & Breach Incidents – 2025

City / Entity	Date	Attack Type	Demand / Impact	Fiscal Impact
City of Pensacola	Jan 2025	LockBit 5.0 Ransomware	\$1.2M ransom demand	\$3.5M recovery costs
City of Tallahassee	Mar 2025	Medusa Ransomware	\$950K ransom demand	\$2.8M system restoration
Florida Department of Health	Apr 2025	RansomHub (Data Exfiltration)	No ransom paid; 100GB leaked	\$5M+ remediation & legal costs
City of Orlando	Jun 2025	Interlock Ransomware	\$1.8M ransom demand	\$4.2M recovery & upgrades
Miami-Dade County Utilities	Sep 2025	Qilin Ransomware	\$2.5M ransom demand	\$6M+ operational disruption
City of Jacksonville	Oct 2025	LockBit 5.0 Ransomware	\$1.4M ransom demand	\$3.9M recovery & downtime
Broward Health	Nov 2025	BlackSuit Ransomware + Data Leak	1.2M patient records exposed; ransom unknown	\$7M+ HIPAA fines & remediation
Palm Beach County Schools	Dec 2025	MedusaLocker Ransomware	\$1.1M ransom demand	\$3M+ recovery & cybersecurity upgrades

FIU - Internal / Private

Key Observations 2025

- **Average ransom demand:** \$1M–\$2.5M for Florida municipalities and public entities; healthcare and education sectors also fall within this range.
- **Financial impact:** Typically **2–3× ransom amount** due to recovery, HIPAA compliance, legal fees, and system hardening.
- **Attack trends:** LockBit 5.0, Medusa, Qilin, Interlock remain dominant; **BlackSuit** and **MedusaLocker** emerged in late 2025 targeting healthcare and K–12.
- **Tactics:** **Double extortion** (encrypt + leak) is standard; attackers increasingly target **critical infrastructure** (utilities, health departments) and **schools** for maximum disruption.
- **Data exposure:** Healthcare breaches involve **massive PHI leaks** (e.g., Broward Health: 1.2M patient records), amplifying regulatory and reputational risk.



Jack D. Gordon
Institute for Public Policy

Linkages & Flows

**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.

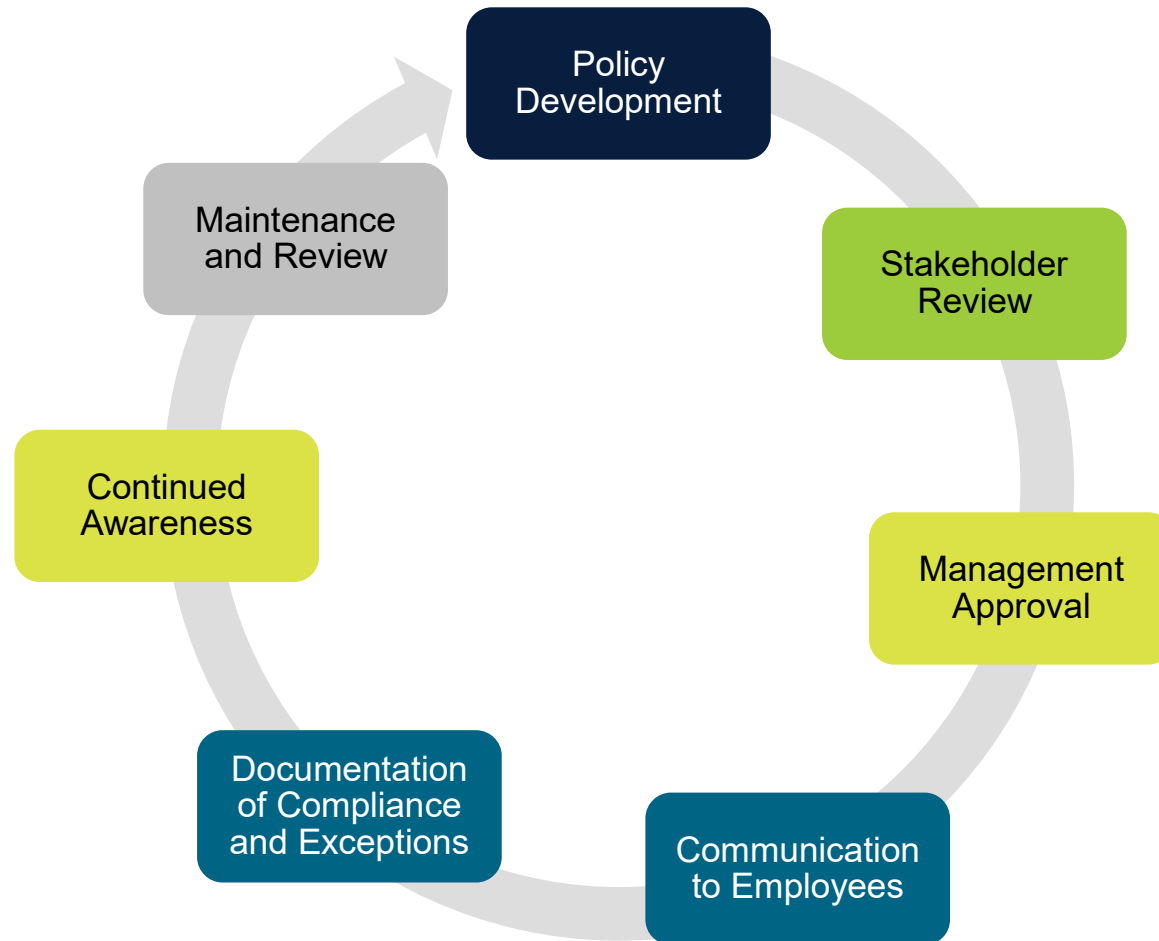
FIU - Internal / Private

Linkages & Flows

- Legislation
 - Federal & state
- Policy
 - Federal, state, county
- Strategy
 - For your organization; what are we going to do
- Plans
 - How you execute your strategy
- Operations
 - Day-to-day activities delivering on your plans

(S)

Policy Development Process



FIU - Internal / Private

(P)

Strategy Development

- General plan to achieve one or more long-term or overall goals under conditions of uncertainty
- Identifies Ends, Ways & Means
 - **Ends:** What do you want to do?
 - What do you need to secure?
 - Who is operating against you
 - What type of operations are they performing?
 - **Ways:** How do you want to do it?
 - Choose a cybersecurity framework
 - Organize yourself
 - **Means:** Resources
 - Hardware
 - Software
 - Wetware (Human)
 - Money

(S)



Objective



Collaboration



Requirements



Planning



Execution



Implementation



Measurement

Defensible Cyber Security Strategy



Governance



**Policies and
Procedures**



**Infrastructures
and Standards**



**People and
Training**



Relationships

(P)

Ten Steps To Develop a Cybersecurity Strategy

Task	Resources
Step 1. Understand your cyber threat landscape.	Industry reports: CISA, Verizon DBIR, etc.
Step 2. Assess your cybersecurity maturity level.	NIST CSF / Third Party Maturity Assessment.
Step 3. Improve cybersecurity program (People, Processes, and Technologies)	NIST Framework (SP-800-53 and CSF)
Step 4. Establish a risk management framework to apply resources that are informed by an assessment of cybersecurity vulnerabilities and cybersecurity threats.	NIST 800-37 - Risk Management Framework for Information Systems and Organizations
Step 5. Prioritize cybersecurity risk management in accordance with the risk level to the organization.	Risk assessment reports, internal audit reports, incident reports, etc.
Step 6. Identify cybersecurity gaps and develop mitigation strategies.	Evaluate current state, i.e., gap assessments, maturity assessments, industry standards, etc.)
Step 7. Define cybersecurity controls that are reasonable and appropriate.	NIST 800-53 and NIST CSF
Step 8. Develop proactive monitoring of security events, continuous monitoring and escalation process.	Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy
Step 9. Develop a cybersecurity incident response plan.	CISA IR Playbooks, NIST SP-800-61, IR partner.
Step 10. Build a continuous user awareness education.	NIST SP-800-50, NIST SP-800-181, SANS

(S)

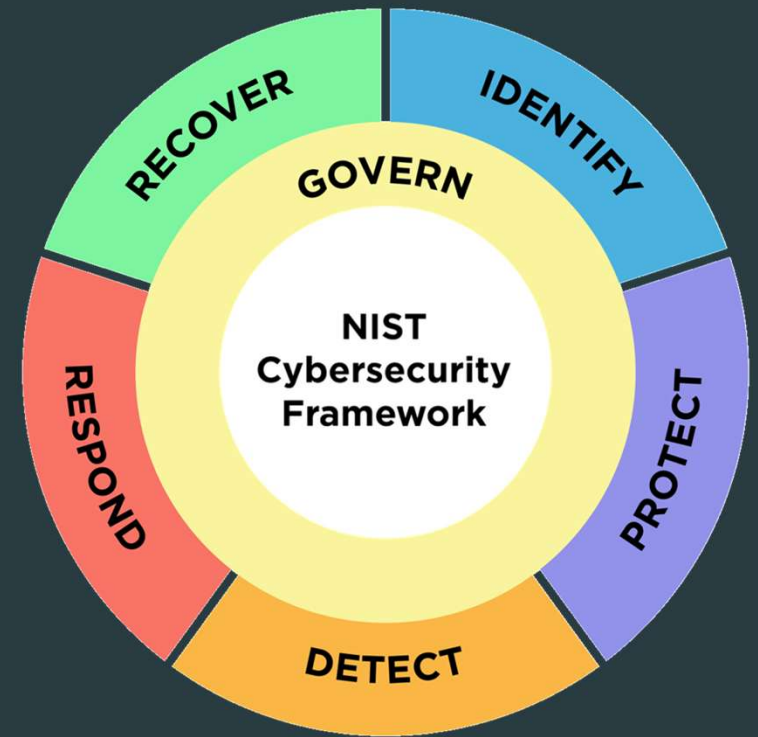
(O)

FIU - Internal / Private



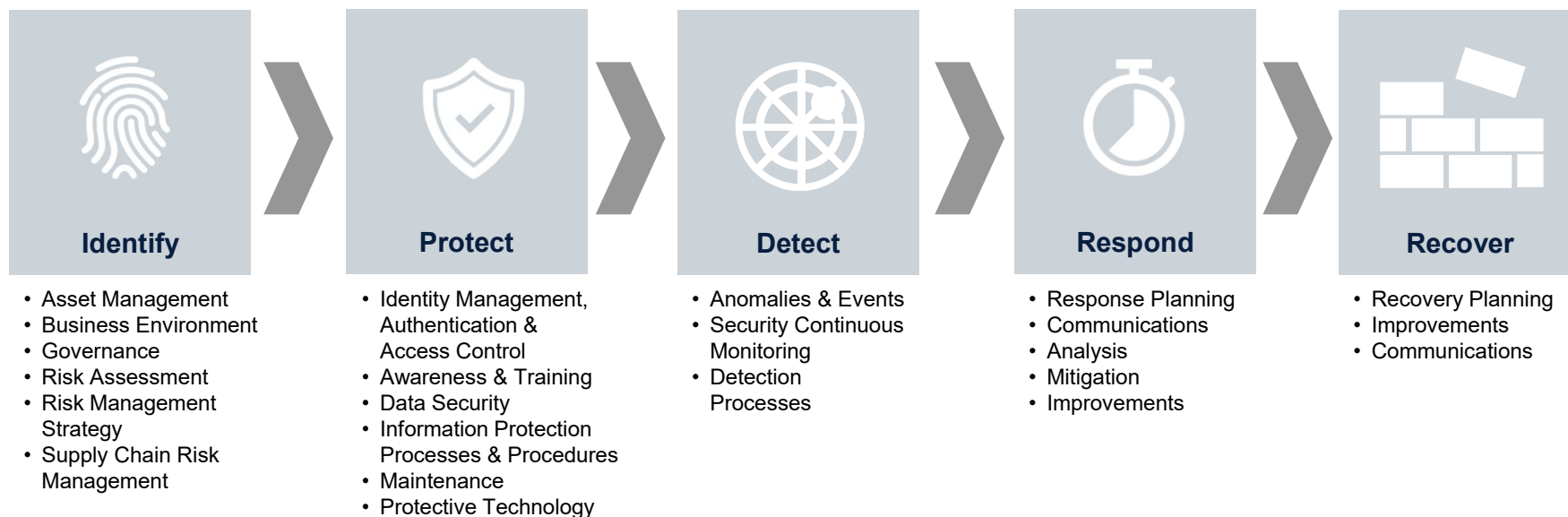
Cybersecurity Framework

nist.gov



NIST Cybersecurity Framework

- **5 Key Pillars** – Holistic and successful program
- Highest level of abstraction – Minimum standards
- **Lexicon** for management to express their cybersecurity management

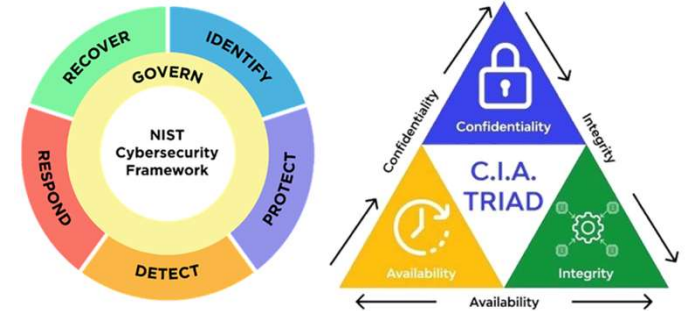


Source: [NIST Cybersecurity Framework](#)

FIU - Internal / Private

Why NIST for local governments?

Fla. Sta. 282.3185(4)(1):

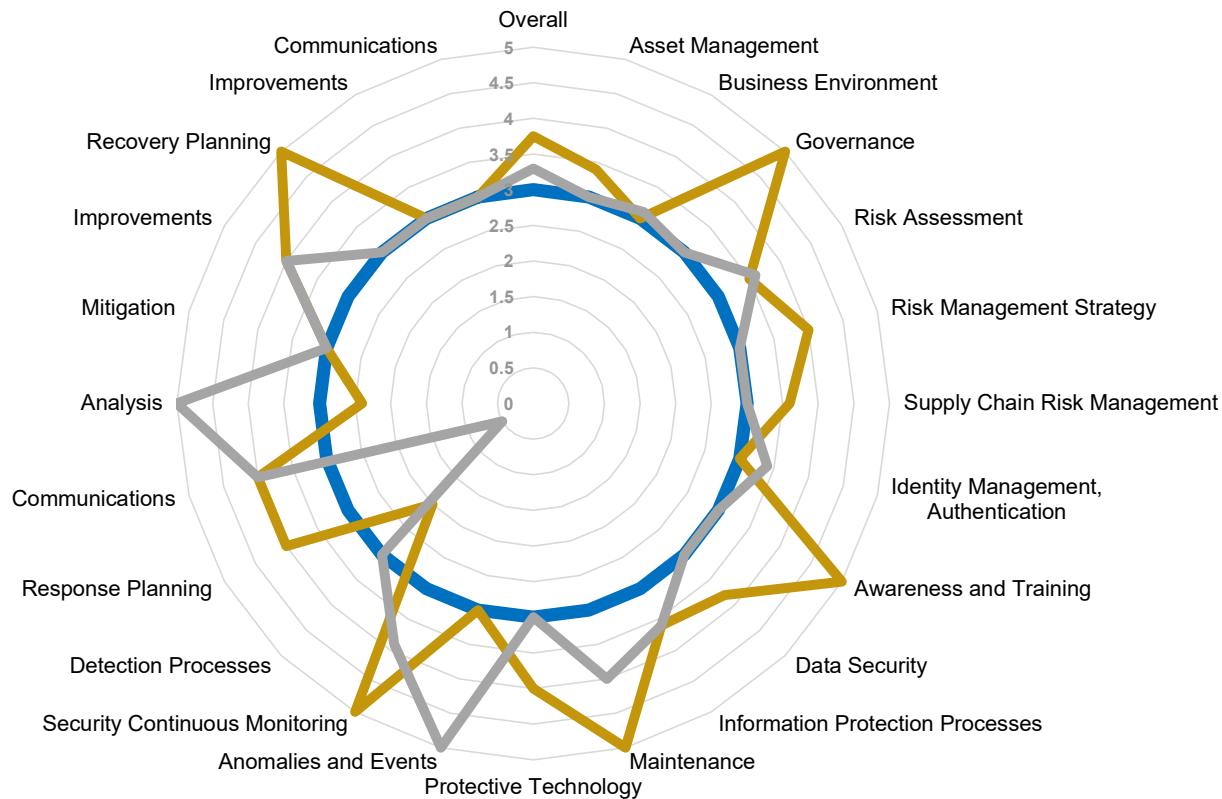


Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the ***National Institute of Standards and Technology Cybersecurity Framework***.

(P)

Maturity Assessment

Sample NIST Cyber Security Framework Maturity Levels



- 5 Optimal
- 4 Managed
- 3 Defined
- 2 Acknowledged
- 1 Initial
- 0 Non-existent

- Target Score
- Policy Score
- Practice Score

(P)

(O)

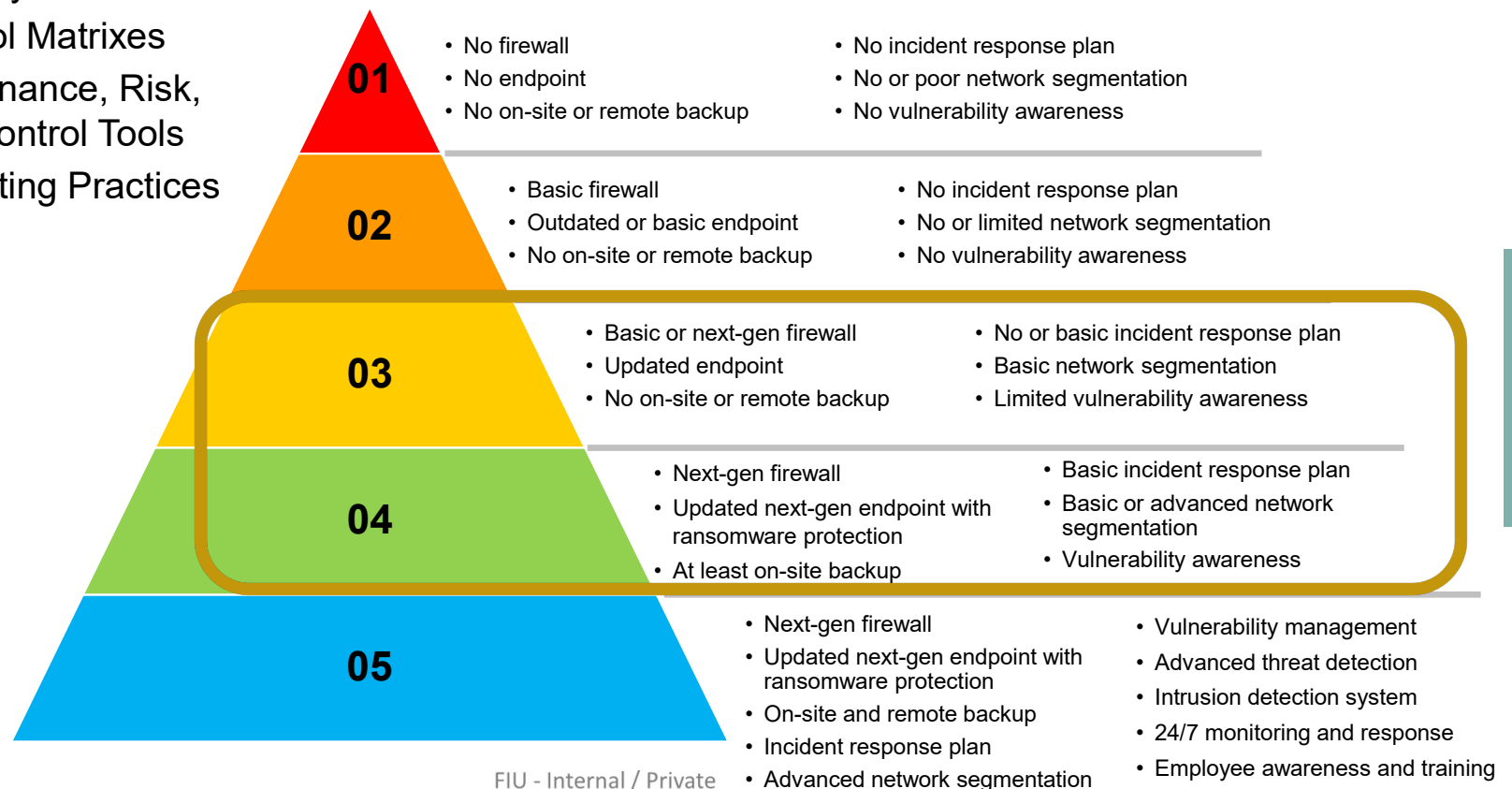
Source: <https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components>

FIU - Internal / Private

Cybersecurity Risk Management (P)

- Maturity Models
- Control Matrixes
- Governance, Risk, and Control Tools
- Reporting Practices

Sample Cybersecurity Maturity Model



FIU - Internal / Private

(P)

FIU

Jack D. Gordon
Institute for Public Policy

FIU

Jack D. Gordon
Institute for Public Policy

THANK YOU!

PLEASE COMPLETE THE COURSE EVAL AT:
wkf.ms/418GQNg



**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 - Internal / Private

FIU

Jack D. Gordon
Institute for Public Policy

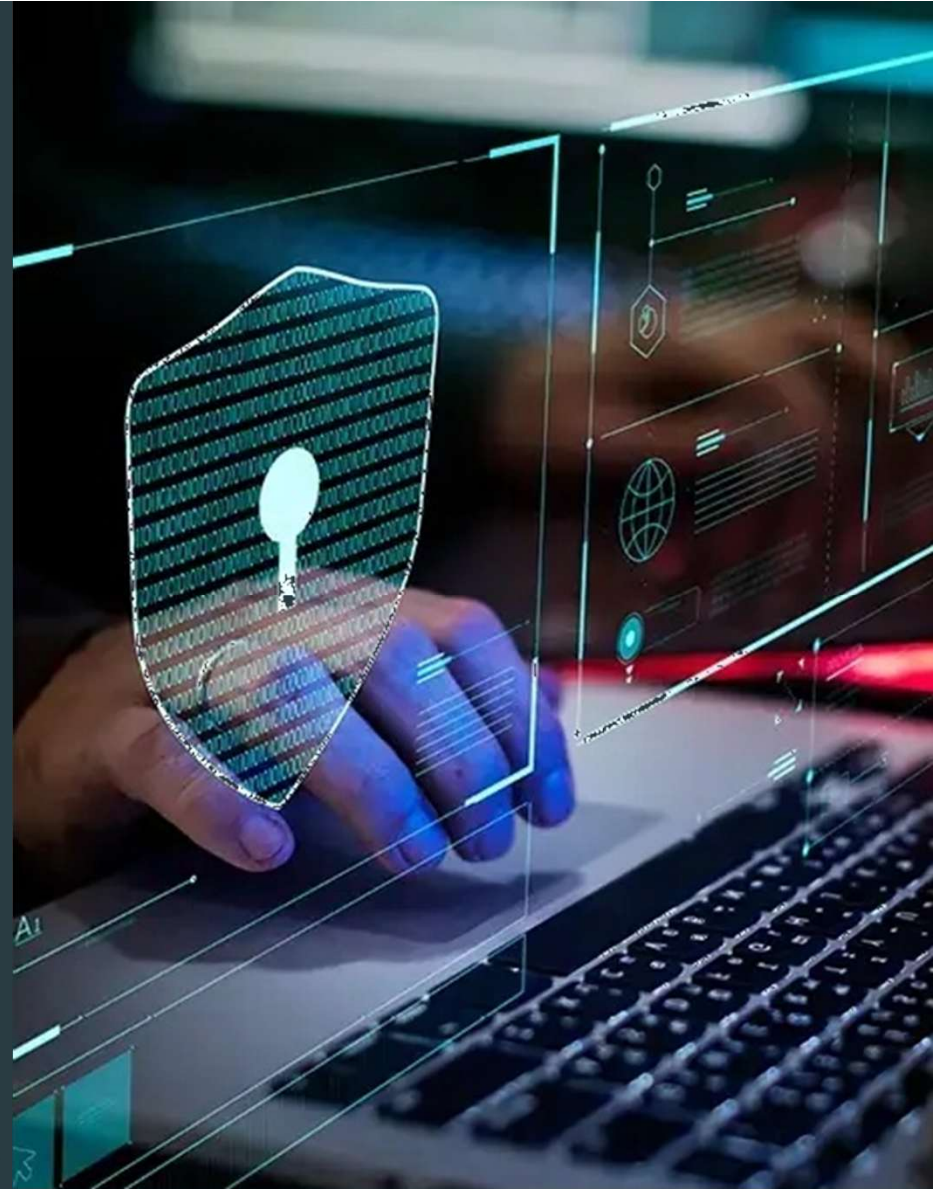
Resources

**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 - Internal / Private



Resources

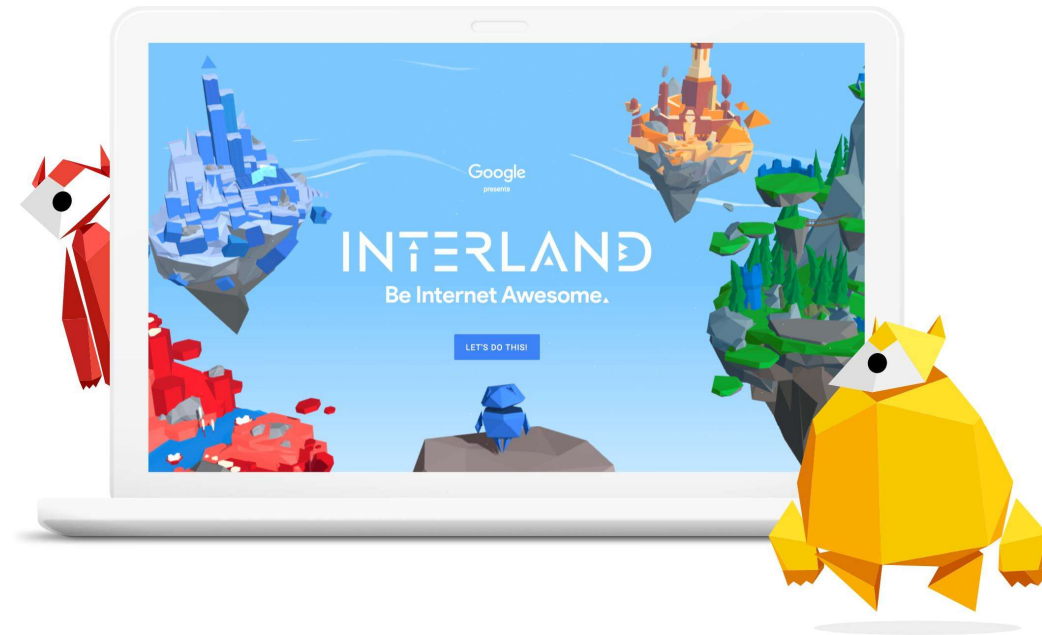
- staysafeonline.org
- cybersmart.org
- connectsafely.org
- sos.fbi.gov
- secureflorida.org
- thefc2.org
- safeandsecureonline.org
- netsmarts.org
- fosi.org
- ikeepSAFE.org



PROTECT YOUR KIDS ONLINE

beinternetawesome.withgoogle.com

Kids can play their way to being Internet Awesome with Interland, an online adventure that puts the key lessons of digital safety into hands-on practice with four challenging games.



Resources (P)

[NIST Cybersecurity Framework \(Critical Infrastructure\), Version 1.1](#)

[NIST Cybersecurity Framework Core \(xls\)](#)

[NIST SP 800-53, Revision 4 \[Summary\]](#)

NIST Special Publication 800-171

- [NIST SP 800-171 Revision 2 \[Summary\]](#)

CSA Cloud Controls Matrix

- [Cloud Controls Matrix v3.0.1 \[Summary\]](#)

CIS Critical Security Controls

- [Critical Security Controls v7.1 \[Summary\]](#)
- [Critical Security Controls v8 \[Summary\]](#)

[NIST SP 800-53, Revision 5 \[Summary\]](#)

- [AC: Access Control](#)
- [AT: Awareness and Training](#)
- [AU: Audit and Accountability](#)
- [CA: Assessment, Authorization, and Monitoring](#)
- [CM: Configuration Management](#)
- [CP: Contingency Planning](#)
- [IA: Identification and Authentication](#)
- [IR: Incident Response](#)
- [MA: Maintenance](#)
- [MP: Media Protection](#)
- [PE: Physical and Environmental Protection](#)
- [PL: Planning](#)

[NIST SP 800-53, Revision 5 \(cont.\)](#)

- [PM: Program Management](#)
 - [PM-1: Information Security Program Plan](#)
 - [PM-2: Information Security Program Leadership Role](#)
 - [PM-3: Information Security and Privacy Resources](#)
 - [PM-4: Plan of Action and Milestones Process](#)
 - [PM-5: System Inventory](#)
 - [PM-6: Measures of Performance](#)
 - [PM-7: Enterprise Architecture](#)
 - [PM-8: Critical Infrastructure Plan](#)
 - [PM-9: Risk Management Strategy](#)
 - [PM-10: Authorization Process](#)
 - [PM-11: Mission and Business Process Definition](#)
 - [PM-12: Insider Threat Program](#)
 - [PM-13: Security and Privacy Workforce](#)
 - [PM-14: Testing, Training, and Monitoring](#)
 - [PM-15: Security and Privacy Groups and Associations](#)
 - [PM-16: Threat Awareness Program](#)
 - [PM-17: Protecting Controlled Unclassified Information on External Systems](#)
 - [PM-18: Privacy Program Plan](#)
 - [PM-19: Privacy Program Leadership Role](#)
 - [PM-20: Dissemination of Privacy Program Information](#)
 - [PM-21: Accounting of Disclosures](#)
 - [PM-22: Personally Identifiable Information Quality Management](#)
 - [PM-23: Data Governance Body](#)
 - [PM-24: Data Integrity Board](#)

[NIST SP 800-53, Revision 5 \(cont.\)](#)

- [PM: Program Management \(cont.\)](#)
 - [PM-25: Minimization of Personally Identifiable Information Used in Testing, Training, and Research](#)
 - [PM-26: Complaint Management](#)
 - [PM-27: Privacy Reporting](#)
 - [PM-28: Risk Framing](#)
 - [PM-29: Risk Management Program Leadership Roles](#)
 - [PM-30: Supply Chain Risk Management Strategy](#)
 - [PM-31: Continuous Monitoring Strategy](#)
 - [PM-32: Purposing](#)
- [PS: Personnel Security](#)
- [PT: Personally Identifiable Information Processing and Transparency](#)
- [RA: Risk Assessment](#)
- [SA: System and Services Acquisition](#)
- [SC: System and Communications Protection](#)
- [SI: System and Information Integrity](#)
- [SR: Supply Chain Risk Management](#)

Resources

- Security Policy Templates

Source: <https://www.sans.org/information-security-policy/>

- The state of ransomware in state and local government

Source: <https://www.scmagazine.com/resource/ransomware/the-state-of-ransomware-in-state-and-local-government#>

- State and Local Government Cyberattacks Timeline

Source: <https://securityintelligence.com/timeline/state-local-government-cyberattacks/year-by-year>

- Examining the Impact of Reactive and Proactive Investments in Cybersecurity

Source: <https://www.healthtechmagazines.com/examining-the-impact-of-reactive-and-proactive-investments-in-cybersecurity/>

- Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Best Practices for Smart Cities

Source: https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf

- FL Cybersecurity Act, Local Government Cybersecurity Act, and Ransomware Incident Compliance

Source: Florida Statutes 218.318 Cybersecurity <https://www.flsenate.gov/laws/statutes/2021/282.318>

- Florida CS/HB 7055 — Cybersecurity

Source: https://www.flsenate.gov/PublishedContent/Session/2022/BillSummary/Military_MS7055ms_07055.pdf

- Sophos: The State of Ransomware in State and Local Government 2022

Source: <https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf>

Resources

- The state of ransomware in state and local government
Source <https://www.scmagazine.com/resource/ransomware/the-state-of-ransomware-in-state-and-local-government>
- Examining the Impact of Reactive and Proactive Investments in Cybersecurity
Source <https://www.healthtechmagazines.com/examining-the-impact-of-reactive-and-proactive-investments-in-cybersecurity>
- CISA Cybersecurity Best Practices for Smart Cities
Source: https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf
- FL Cybersecurity Act, Local Government Cybersecurity Act, and Ransomware Incident Compliance
Source Florida Statutes 218.318 Cybersecurity <https://www.flsenate.gov/laws/statutes/2021/282.318>
- Florida CS/HB 7055 — Cybersecurity
Source https://www.flsenate.gov/PublishedContent/Session/2022/BillSummary/Military_MS7055ms_07055.pdf

(S)

(P)

(O)

FIU

Jack D. Gordon
Institute for Public Policy

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.