

FIU

Jack D. Gordon
Institute for Public Policy



Securing the Future: Cyber Defense for Public Finance Leaders

Hosted by Florida Government Finance Officers Association (FGFOA)

January 17, 2025

**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.



Mike Asencio

Acting Director, Cybersecurity
Jack D. Gordon Institute for Public Policy
Florida International University

Cyber Security Leadership & Strategy Course Sign In



Learning Objectives

1. **Understand Key Cybersecurity Requirements:**

Gain a clear understanding of the Florida Local Government Cybersecurity Act (F.S. 282.3185) and its impact on public finance entities, including compliance and operational expectations.

2. **Identify and Address Cybersecurity Threats:**

Recognize the unique risks faced by government finance systems and implement effective measures to protect sensitive data and resources.

3. **Strengthen Leadership in Cyber Defense:**

Equip finance leaders with strategies to promote security awareness, align operations with statutory requirements, and effectively respond to cybersecurity incidents.

FIU

Jack D. Gordon
Institute for Public Policy

Cybersecurity Threat Landscape

**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

Role of Leaders in Cybersecurity

Senior Leaders

- Identify what is important to the organization (what needs to be protected)
- Understand legislation and policies
- Choose internal policies (presented by CIO/CISO)
- Identify Ends (what do we want to do)
- Approve Ways (how are we going to do it)
- Provide Means (resources, budget)
- Communicate to the enterprise
 - Why is cybersecurity important
 - Why everyone has to follow good practices (e.g. cyber hygiene)
 - Create a culture of cyber security
- Monitor CIO/CISO performance during planning and operations
- Ensure reporting – needs a decision!
- Strategic Communications

CIO / CISO / IT Director

- Identify legislation and policies
- Recommend policies to senior leaders
- Recommend a cybersecurity framework
- Take Ends identified by senior leaders
- Recommend Ways to senior leaders
- Manage Means provided by senior leaders
- Keep senior leadership updated

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**

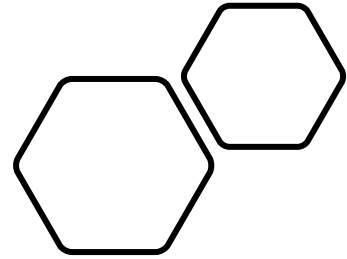


“City of Atlanta officials highlighted the importance of protecting government data and information, and of bringing discipline to an agency’s approach to cybersecurity.”

(S)

(P)

(O)



Costa Rica Cyber attacks April/May 2022

April 17, 2022, a ransomware attack began against nearly 30 institutions of the government of Costa Rica:

- Ministry of Finance (MOF)
 - Ministry of Science, Innovation, Technology and Telecommunications (MICITT)
 - National Meteorological Institute
 - State internet service provider RACSA
 - Costa Rican Social Security Fund (*Caja Costarricense de Seguro Social, CCSS*)
 - Ministry of Labor and Social Security
 - Fund for Social Development and Family Allowances, and the Administrative Board of the Municipal Electricity Service of Cartago
- The attack consisted of infections of computer systems with ransomware, defacement of web pages, theft of email files and attacks on the Social Security human resources portal, as well as on its official Twitter account
- Pro Russian group **Conti** used compromised credentials and demanded a US\$10 million ransom in exchange for not releasing the information stolen.
- Losses to the productive sector on the order of US\$30 million per day

Costa Rica Cyber attacks April/May 2022

- By Apr 22 they have detected 35,000 malware communication requests, 9,900 phishing incidents, 60,000 attempts to take remote control of IT systems, and 60,000 attempts to mine cryptocurrencies using the computer infrastructure of the first 100 state institutions intervened
- May 8 new President assumes power, declared a state of national emergency & ordered the Presidency of the Republic to take control of the coordination of the national response, in lieu of the National Emergency Commission “we have 27 institutions attacked and 9 institutions very affected, including the Ministry of Finance, which is the one that receives the income and makes the expenses of the State. They want to drown us through the financial system of the State's public finances.”
- Nearly two months after the original attack, on June 11, the MOF announced that the ATV tax system would be restarted on June 13 so that Costa Ricans could make their payments.
- On June 24, two other systems disabled by Conti attacks were restored: TICA (*Tecnología de Información para el Control Aduanero*, Customs Control Information Technology) and Exonet, a platform used to manage and process tax exemption requests.

Costa Rica Cyber attacks April/May 2022

April 20, Conti published 5 GB of information stolen from the Ministry of Finance on one device in the Ministry of Finance network. *Radiografía Costarricense S.A. (RACSA)*, a state internet service provider, was also attacked

April 21, Conti Group attacked the servers of the Ministry of Labor and Social Security, as well as the Social Development and Family Allowances Fund. President reminds everyone they need to report everything to Computer Security Incident Response Center (CSIRT-CR) even if it is considered under control

April 23, Conti Group attacked the Administrative Board of the Municipal Electrical Service of Cartago

April 25, Conti announced that it would shift its strategy from attacking state institutions to focus on large companies in the private sector

April 26, the MICITT reported that the website of the Sede Interuniversitaria de Alajuela and that they had repelled an attempt to breach the servers of the Instituto de Desarrollo Rural (Rural Development Institute)

April 29, the government reported a hacking attempt to the Ministry of Economy, Industry and Commerce

April 30 hacking attempts at National Liquor Factory and the municipalities of Turrialba and Golfito

May 2 another hacking attempt was rebuffed at the Ministry of Justice and Peace (MJP)

May 3 unsuccessful cyberattacks were reported on the municipalities of Garabito and Alajuelita, as well as on the San José Social Protection Board [es], a national charitable organization that administers the country's national lottery.

May 4, MICITT reported hacking attempts to the National Education Loan Commission and one more to the Cartago University College

Hive Operations in Costa Rica

May 31 Hive Ransomware Group attacked the Costa Rican Social Security Fund, forcing the institution to turn off all of its critical systems. CCSS detected anomalous information flows in its systems and began to receive reports from different hospitals of unusual behavior in various computers; it immediately proceeded to turn off all its critical systems. CCSS officials described the attack as "**exceptionally violent**"

Financial areas of the CCSS were unable to use systems including the Centralized Collection System (SICERE), the Disability Control and Payment Registry (RCPI), and the Integrated Voucher System (SICO). Offices and administrative areas were unable to use computers.

May 31:

- 4,871 users missed their medical appointments

- another 12,000 missing appointments the next day.

- Laboratory service was the most affected, with only 45 percent operating normally and 48 percent partially affected.

Review of 108 health establishments showed that 96% of hospital services operated with a contingency plan, 18% of outpatient consultations were partially affected, 19% of radiology and medical imaging services were partially affected, and 37% of pharmacy services were affected.

Hive Operations in Costa Rica

June 1:

Effects of the attack were 27 times greater than what was reported on the first day
More than 800 servers and 9,000 end-user computers were affected
Impossible to restore all systems within a week as initially planned.

On June 2, the Hive Ransomware Group requested \$5 million in bitcoin so that the CCSS could get its services back.

On June 4, the Superintendency of Pensions (SUPEN) announced the suspension until further notice of the possibility of freely transferring complementary pension funds.

Sector- specific cyber threats

Economic growth, Finance, and trade

300 global CEOs cited the lack of cybersecurity as the single greatest threat to the global economy over the next decade

Small and medium-sized enterprises (SMEs) generate a significant portion of GDP. SMEs:

- Tend to have low levels of cybersecurity

- Are common targets for cyberattacks including cybercrime

Level of cybersecurity of institutions deemed critical to the function of the economic and financial vitality of a country: ministries of finance, central banks, and large banks

The loss of data or cost of recovering from the attack could be detrimental to a country's economy, causing financial harm to a range of actors including, but not limited to, the national government, businesses, or individual

Question:

What was a critical failure in Atlanta's response to their cyberattack?

- A. Lack of incident response plan
- B. Overfunding cybersecurity
- C. No financial impact
- D. Immediate resolution of the attack

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

Types of Cyber Operations

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 	<div style="background-color: #ffff00; padding: 5px; display: inline-block;">Requires attribution!</div>

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

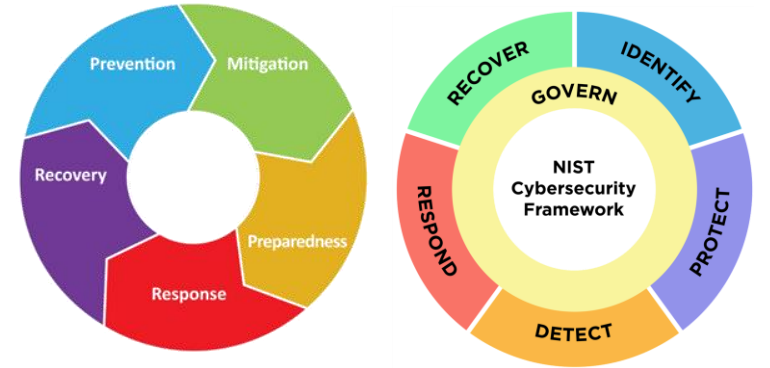


FEMA	NIST	Good for
Prevent	Identify	Strategies and plans for the inevitable
Protect		Cyber hygiene to prevent 80-90%
Mitigate	Detect	Detect operation to catch the 10-20%
Respond		
Recover		

Governance

Governance:

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



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

Question:

Which of the following is the most common cyber threat faced by local governments?

- A. Ransomware
- B. Social engineering
- C. Phishing attacks
- D. Insider threats

Most Common Cyber Operations Techniques

Entry Operations

- Phishing
- Spear Phishing
- Whaling
- SMSHING
- 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

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	Intel	
		Crime								
	Attack	Attack	Attack	Attack	Attack	Attack		Attack	Attack	
Business	Info	N/A	Info	Intel	Intel	Intel	Intel	Info	N/A	
	Intel		Intel					Intel		Intel
			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	
Populations	Info	N/A	N/A	N/A	N/A	N/A	Info	Info	N/A	
	Intel						Intel	Intel		

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		

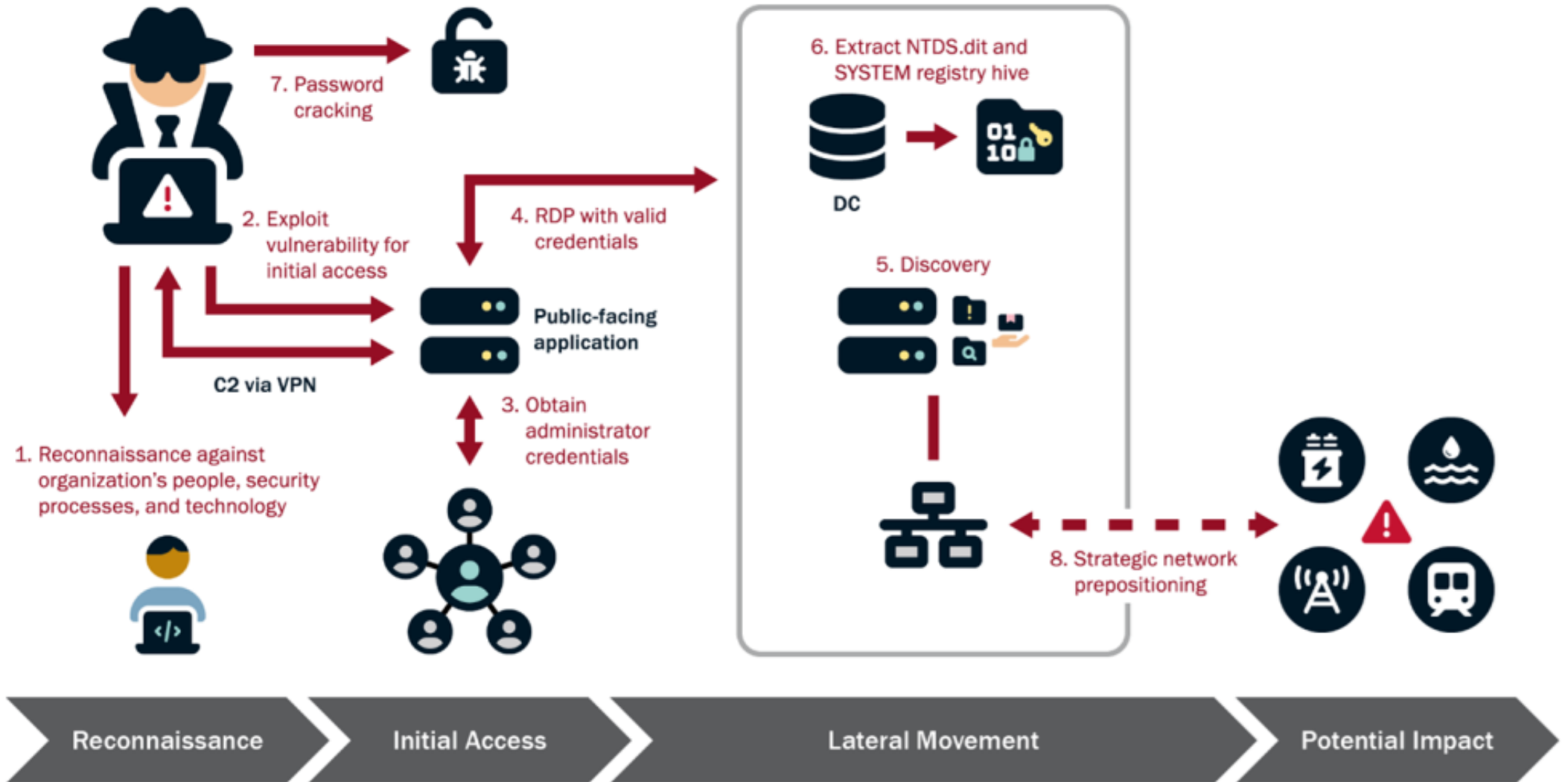
(T)

(S)

(P)

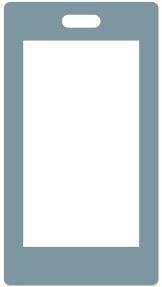
(O)

Living Off the Land (LOTL) Attacks



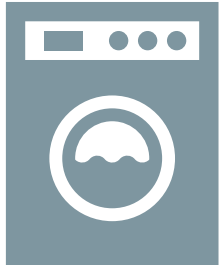
SOURCE: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA

Major Threats



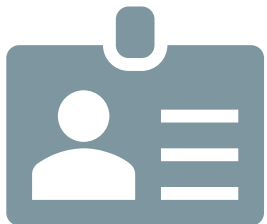
Individual: Smart phone

- End User Licensing Agreement (EULA)



Family: Internet of Things

- Lack of security allows access to router



Organization: Insider Threat

- People are the weak point

What is Ransomware

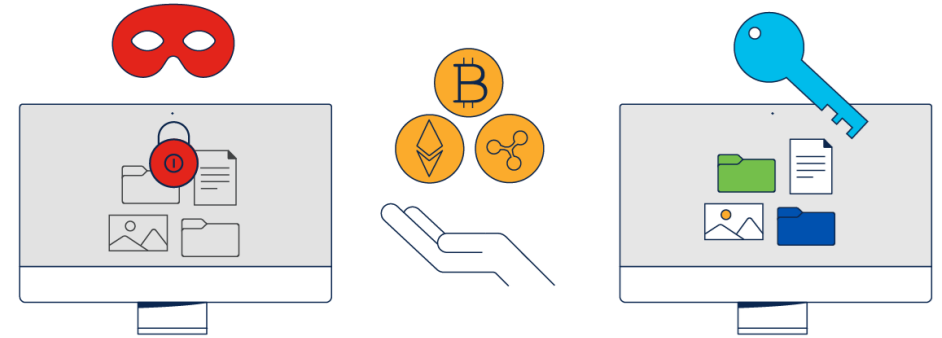
(T)

- 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.



(P)

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>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

What happened.

On February 19, 2024 penetration testing of two of my servers took place, at 06:39 UTC I found an error on the site 502 Bad Gateway, restarted nginx - nothing changed, restarted mysql - nothing changed, restarted PHP - the site worked. I didn't pay much attention to it, because for 5 years of swimming in money I became very lazy, and continued to ride on a yacht with titsy girls. At 20:47 I found that the site gives a new error 404 Not Found nginx, tried to enter the server through SSH and could not, the password did not fit, as it turned out later all the information on the disks was erased.

Due to my personal negligence and irresponsibility I relaxed and did not update PHP in time, the servers had PHP 8.1.2 version installed, which was successfully penetration tested most likely by this CVE <https://www.cvedetails.com/cve/CVE-2023-3824/> , as a result of which access was gained to the two main servers where this version of PHP was installed. I realize that it may not have been this CVE, but something else like 0day for PHP, but I can't be 100% sure, because the version installed on my servers was already known to have a known vulnerability, so this is most likely how the victims' admin and chat panel servers and the blog server were accessed. The new servers are now running the latest version of PHP 8.3.3. If anyone recognizes a CVE for this version, be the first to let me know and you will be rewarded.

<https://www.linkedin.com/pulse/lockbit-oye-jitu-mani-das-cism-cissp--2u3mf/>



\$12.5 Billion

Losses in 2023



2,412

Average complaints received daily

2021
2019
2018
2017
2016

758,000+

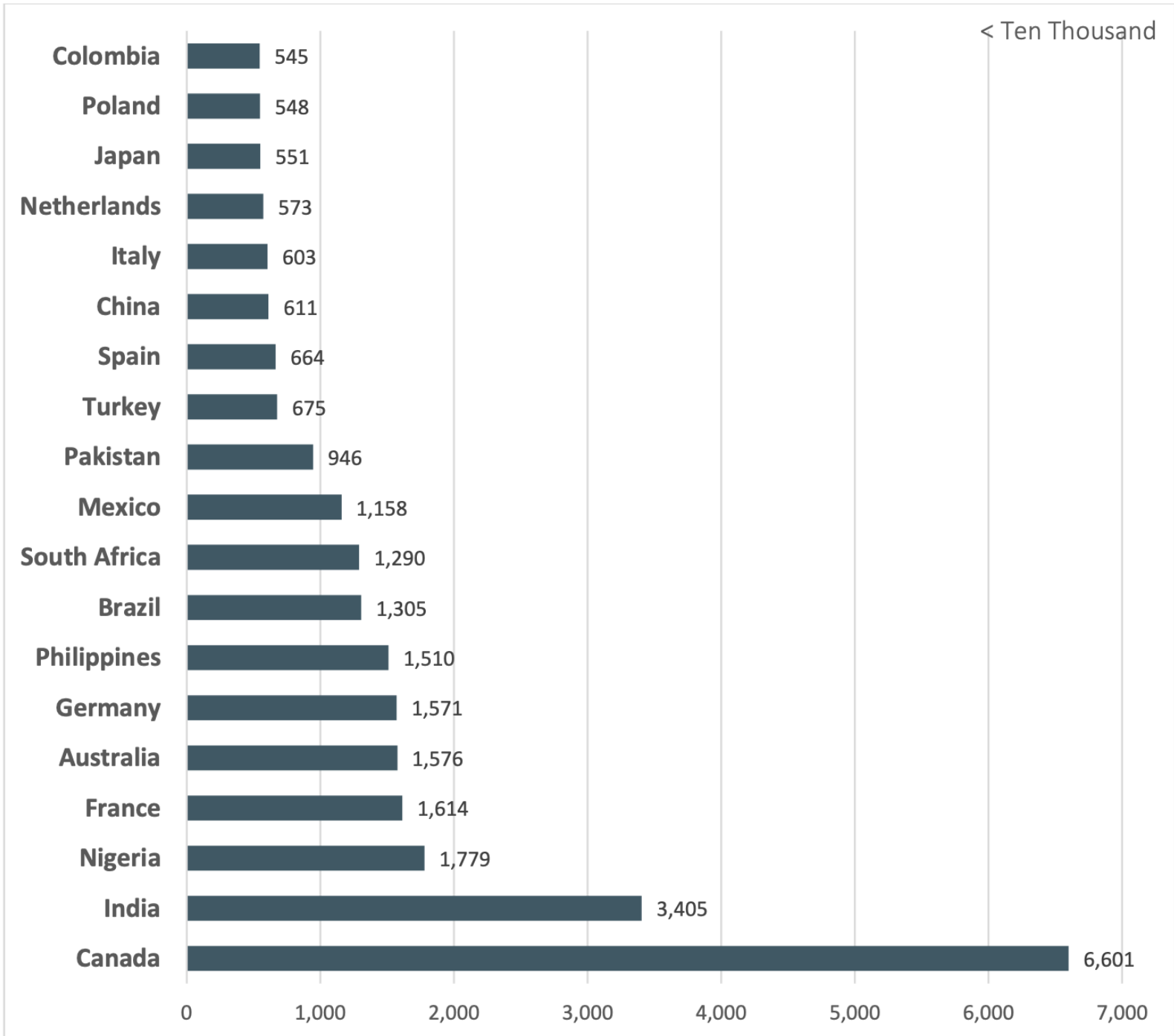
Average complaints received per year (last 5 years)

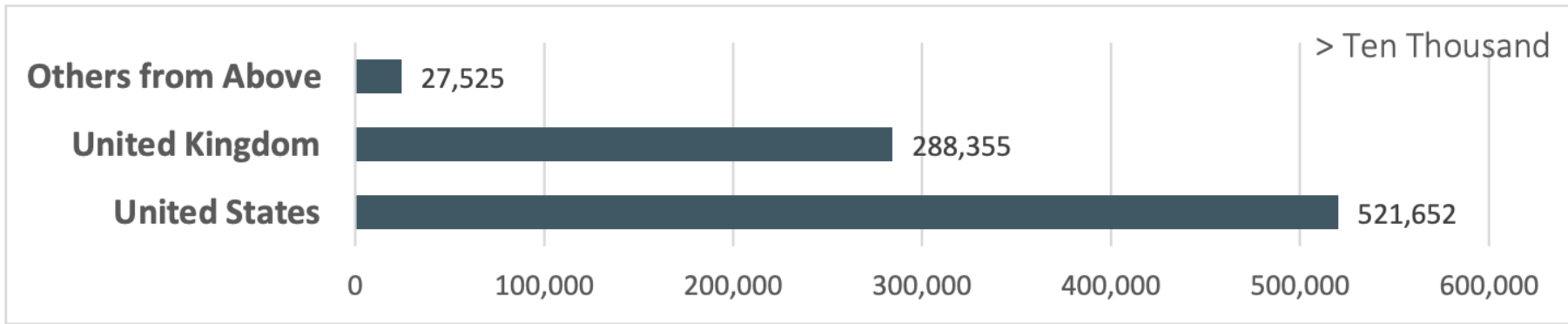


Over 8 Million

Complaints reported since inception

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf





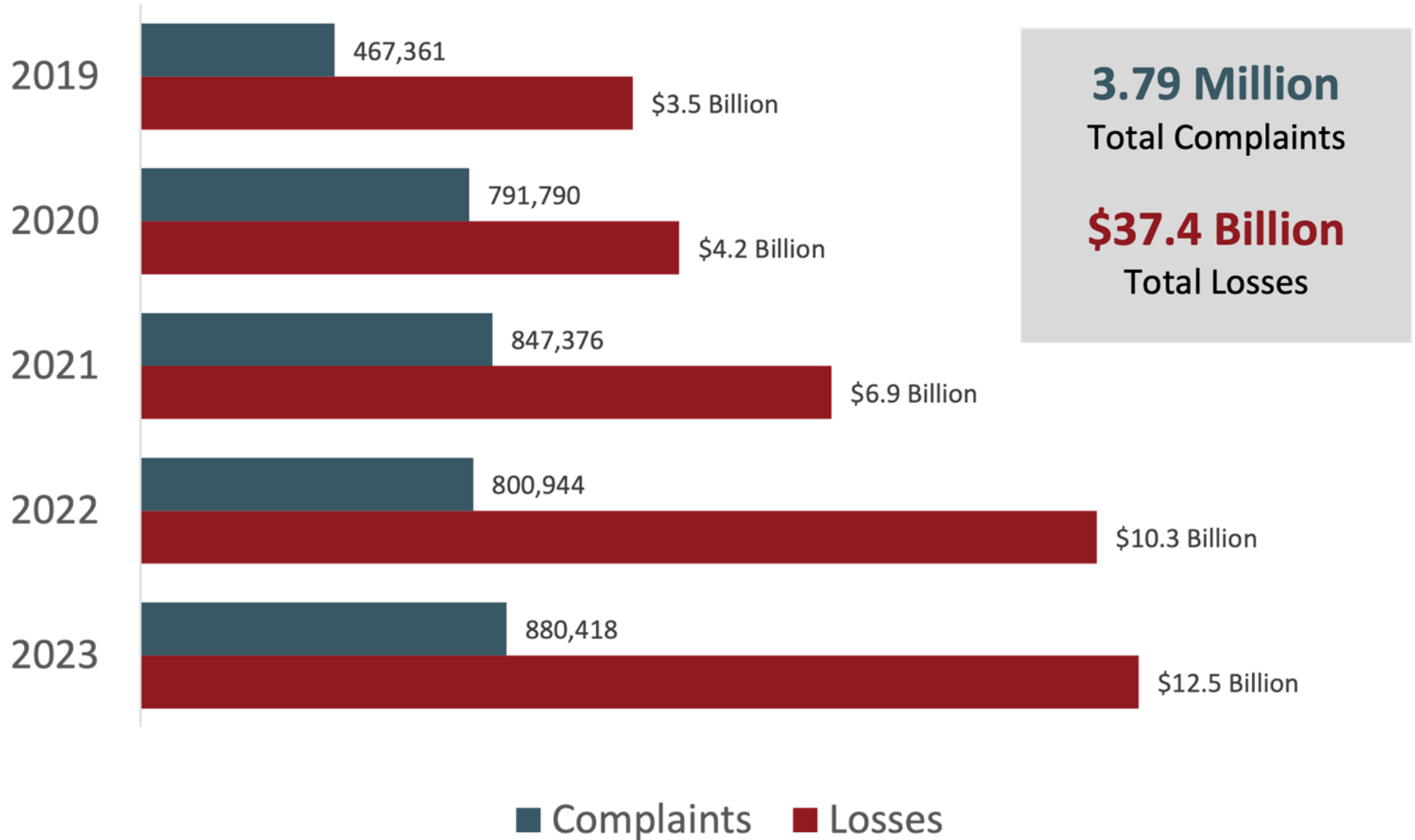
Complaints per State*

Rank	State	Complaints
1	California	77,271
2	Texas	47,305
3	Florida	41,061
4	New York	26,948
5	Ohio	17,864
6	Arizona	16,584
7	Pennsylvania	16,407
8	Illinois	15,783
9	Michigan	14,784
10	Washington	14,600

Losses by State*

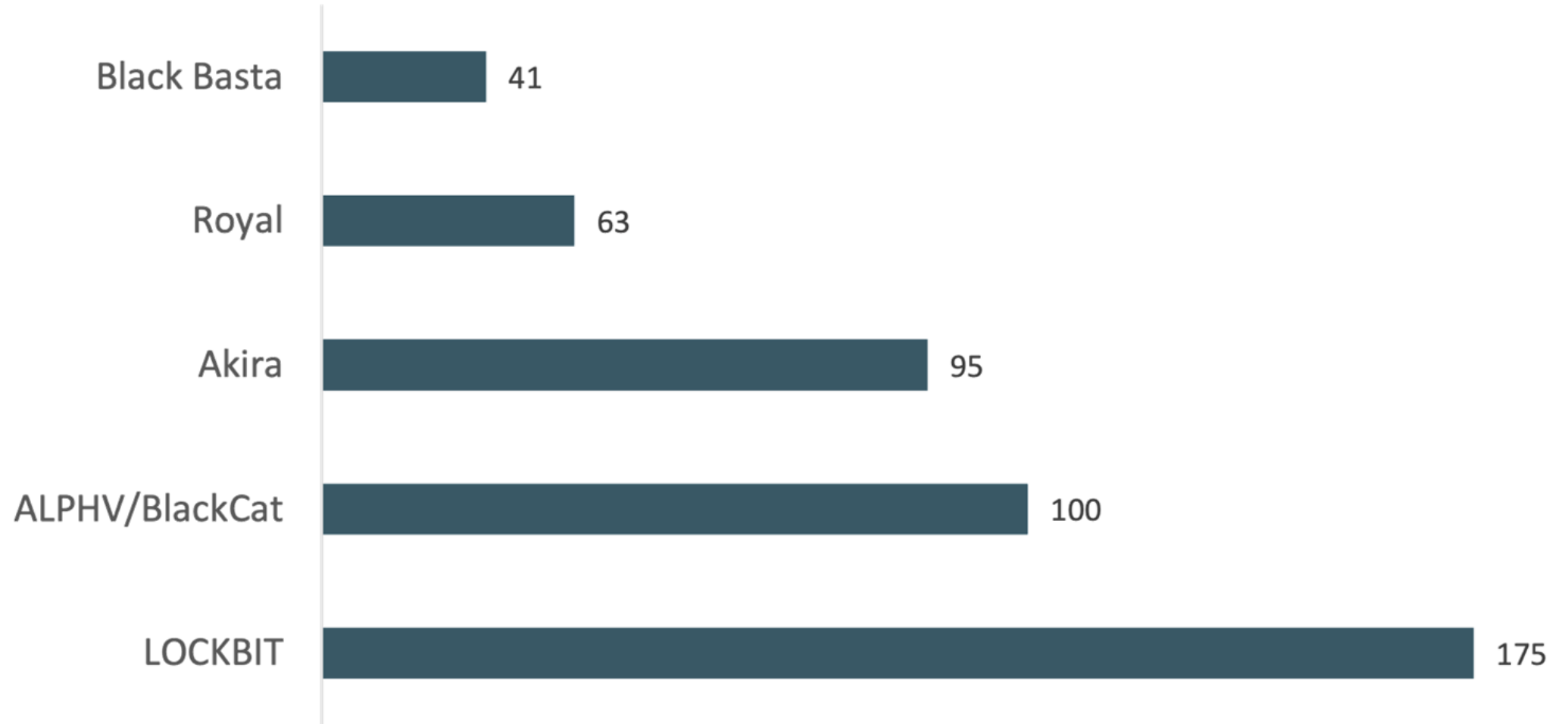
Rank	State	Loss
1	California	\$2,159,454,513
2	Texas	\$1,021,547,286
3	Florida	\$874,725,493
4	New York	\$749,955,480
5	New Jersey	\$441,151,263
6	Pennsylvania	\$360,334,651
7	Illinois	\$335,764,223
8	Arizona	\$324,352,644
9	Georgia	\$301,001,997
10	Washington	\$288,691,091

Complaints and Losses over the Last Five Years*



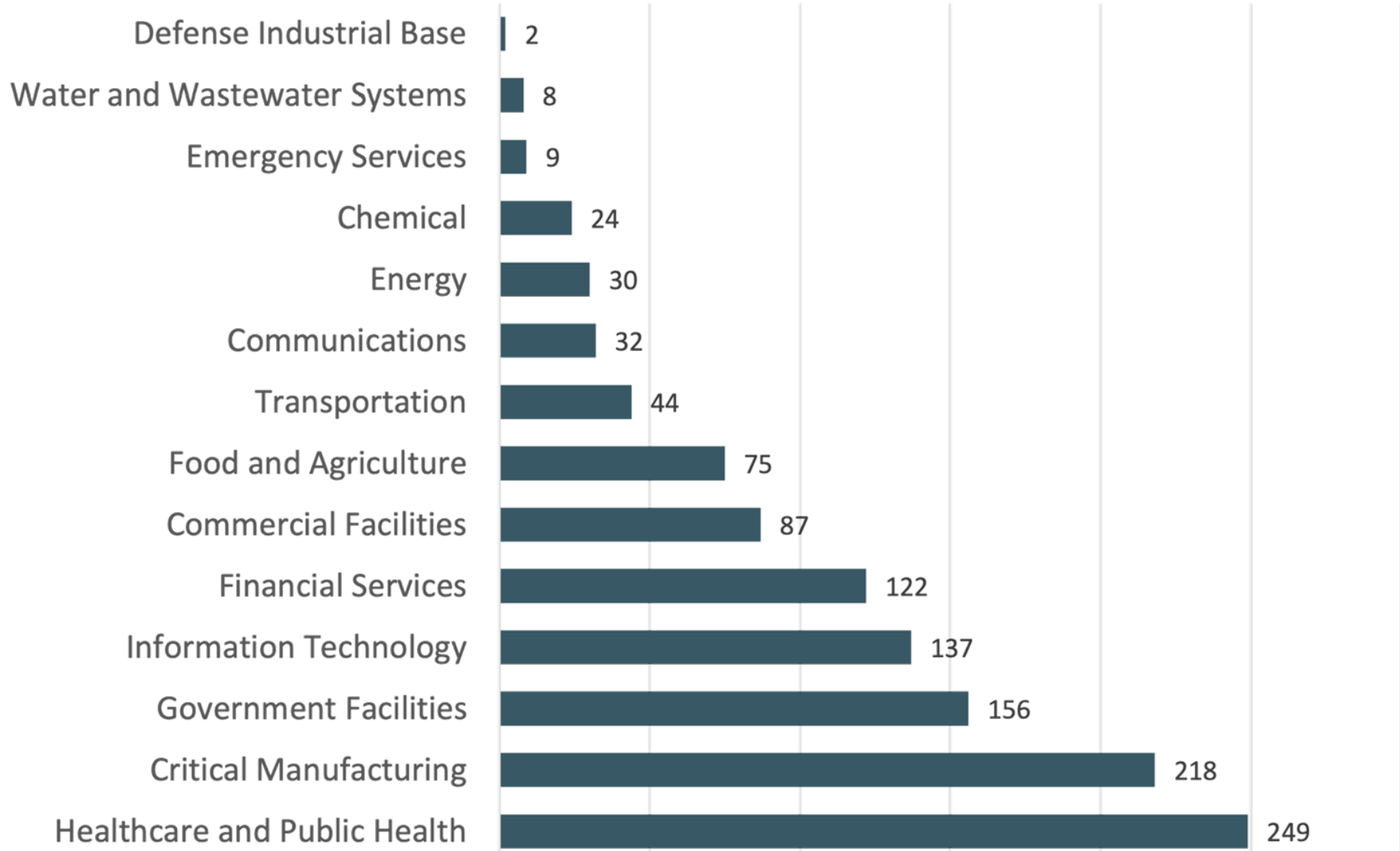
Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Top Ransomware Variants Affecting Critical Infrastructure 2023



Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Infrastructure Sectors Affected by Ransomware



Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

How is ransomware different from other cyber operations?

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

Question:

What is the best immediate action finance leaders can take to improve cybersecurity?

- A. Schedule employee training
- B. Review the compliance checklist
- C. Develop an incident response plan
- D. All of the above

Ransomware US December 2023

[Great Valley School District](#) in Pennsylvania
[Ongoing Operations](#) who supports ~60 credit unions in the US
US Payments Giant [Tipalti](#)
[Hermon School Department](#) Maine
[Austal USA](#) a shipbuilder for the US Navy
[St Johns River Management District](#) a regulatory agency in Florida.
[Dameron Hospital](#) in California
[Taylor University](#) in Indiana
[Henry County Schools](#) in Georgia
[Sweetwater High School District](#) in California
[Stanley Steemer](#)

[Glendale Unified School District](#) in California
[Fred Hutchinson Cancer Center](#) in Seattle
[Greater Richmond Transit Company \(GRTC\)](#) in Virginia
[Hinsdale School District](#) in Vermont
Washington-based drug store chain [Hi-School Pharmacy](#)
[Heart of Texas Behavioral Health Network](#),
[Americold](#)
[Campbell County Schools](#) in Kentucky
[Memorial Sloan Kettering Cancer Center](#) in New York City
[City of Defiance](#) in Ohio
[KraftHeinz](#) food corporation

70 total; 45 US, 25 international

Source: <https://www.blackfog.com/ransomware-report/>

Ransomware US December 2023

[Foursquare Healthcare](#) in Texas
Hotel chain [Red Roof](#)
US Online education platform [Wondrium](#)
[Petersen Health Care](#) in Illinois
[Covenant Care](#) in the western US
[Neurology Center of Nevada](#)
[Milton Town School District](#) in Vermont
[Liberty Hospital](#) in Missouri
[Clay County](#) in Minnesota
[Integrus Health](#) in Oklahoma
[Cullman County Revenue Commissioner](#) in Alabama
The [Ohio Lottery](#)
[American Alarm and Communications \(AAC\)](#).
[New York School of Interior Design](#)

US division of Xerox Business Solutions (XBS) of [Xerox Corporation](#).
[Newfound Area School District](#) in Virginia
[Viking Therapeutics](#) in Vermont
[VF Corporation](#) in Colorado owners of brands like Supreme, Vans, Timberland, and The North Face
Specialty pharmacy chain [BioMatrix](#) in Florida
[ESO Solutions](#) in Texas who provides software to hospitals and EMS
[Richmont Graduate University](#) in Georgia
[National Amusements](#) in Massachusetts
US-based [Ultra Intelligence and Communications](#)

44 total; 20 Local/Regional, 19 national, 5 international

Source: <https://www.blackfog.com/the-state-of-ransomware-in-2022> = 376 publicly reported Ransomware operations

Ransomware International December 2023

UK premium independent retailer [Jules B](#)
[HTC Global Services](#) IT services and consultancy
firm in India

[Hangzhou Great Star Industrial Company](#) in
China

[Ho Chi Minh City Energy Corporation](#)
(EVNHCMC) a subsidiary of Vietnam Energy

[La Prensa](#) a newspaper in Nicaragua

Canadian multinational retailer [Aldo Shoes](#)

[Deutsche Energie-Agentur \(Dena\)](#)

Munich-based games developer [Travian Games](#)

UK travel company [Hotelplan UK](#)

[Decina](#), an Australian bathroom product
manufacturer

Sony-owned game developer [Insomniac Games](#)

[Blue Waters Products Ltd](#) in Trinidad

[GOLFZON](#) a world-renowned golf simulator
manufacturer in Korea

[AMCO Proteins](#) in the UK

One of the world's largest law firms [CMS](#) in
Europe

[University of Buenos Aires](#)

Indian IT company [HCL Technologies](#)

UK accountancy firm [Xeinadin](#),

[Abdali Hospital](#) in Jordan,

German hospital network, [Katholische
Hospitalvereinigung Ostwestfalen \(KHO\)](#),

[Israel Electric Corporation](#).

[National Insurance Board of Trinidad and Tobago
\(NIBTT\)](#),

Japanese car manufacturer [Nissan](#)

[Yakult Australia](#)

[Elektroprivreda Srbije \(EPS\)](#) in Serbia

FL Cybersecurity Advisory Council on Cyber Hygiene

(T)

- **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

(P)

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



Jack D. Gordon
Institute for Public Policy

Linkages & Flows

**CYBER
FLORIDA**
FIRSTLINE

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

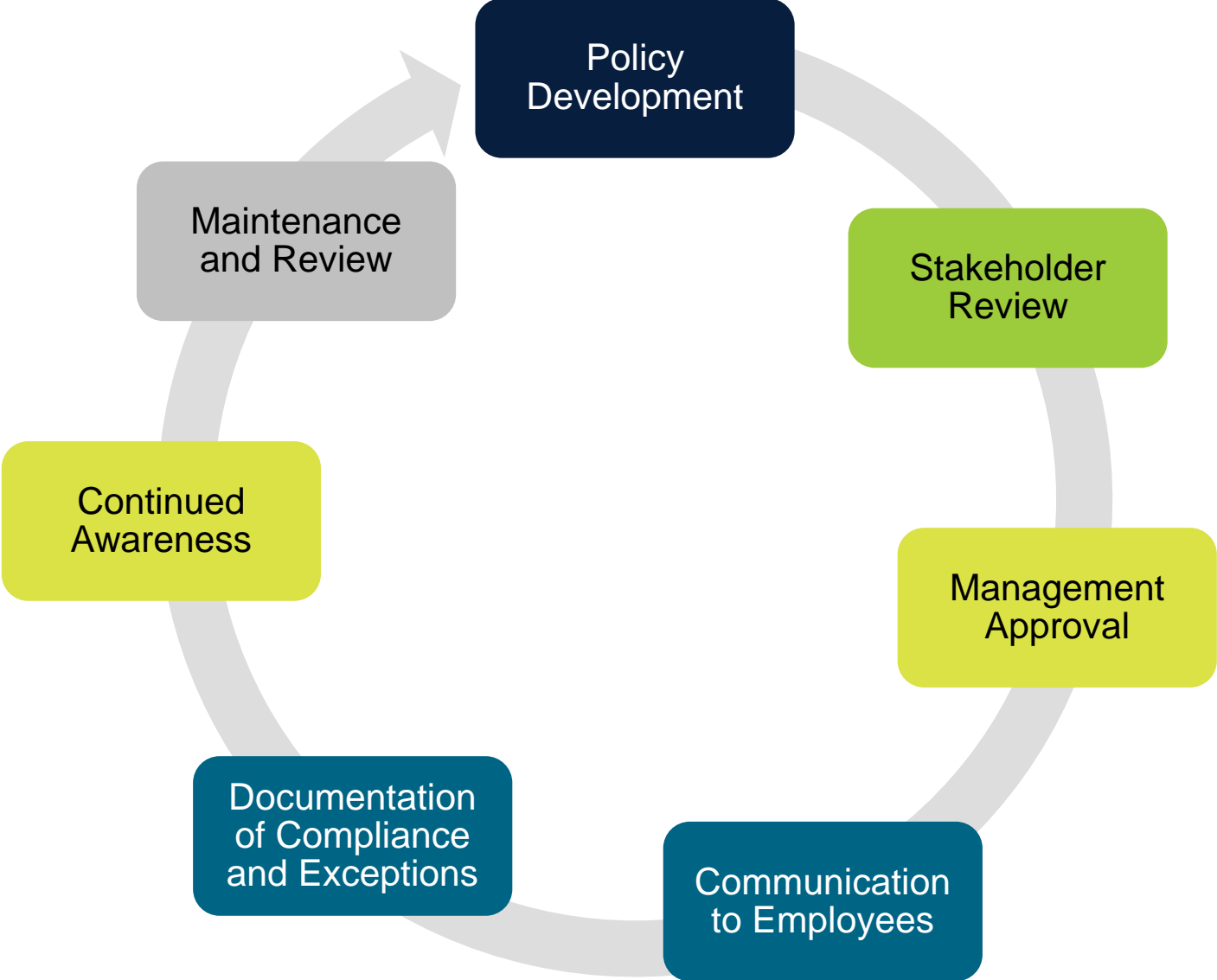
This program is provided at no
cost to Florida public-sector
employees through the
Cyber Florida FirstLine initiative
funded by the Florida Legislature
and led by Cyber Florida at USF.

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



(P)

Question:

What percentage of cyber threats can be mitigated with good cyber hygiene practices?

- A. 30-40%
- B. 50-60%
- C. 70-80%
- D. 80-90%

Strategy

- 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)

Defensible Cyber Security Strategy



Governance



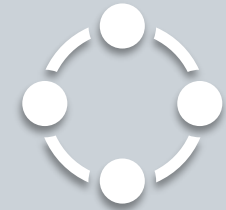
**Policies and
Procedures**



**Infrastructures
and Standards**



**People and
Training**



Relationships

(P)

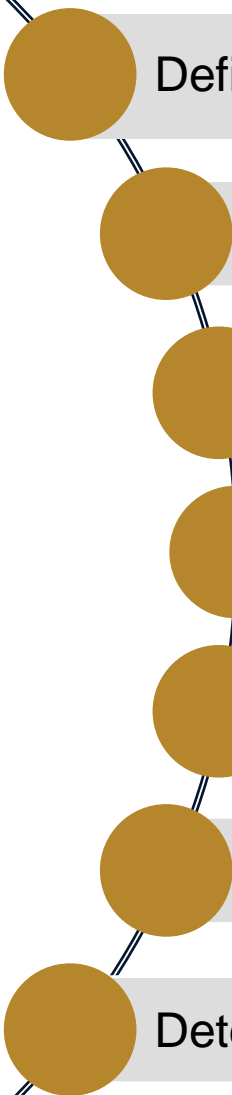
Ten Steps To Develop a Cybersecurity Strategy

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)

Cybersecurity Strategy Goals

- 
- Define the desired state
 - Determine the current state
 - Gap analysis – current versus desired states
 - Identify threats
 - Identify the “how” – set up for a plan
 - Design monitoring and metrics
 - Determine resources required

(S)

FIU

Jack D. Gordon
Institute for Public Policy

NIST

**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.

Why NIST for local governments?

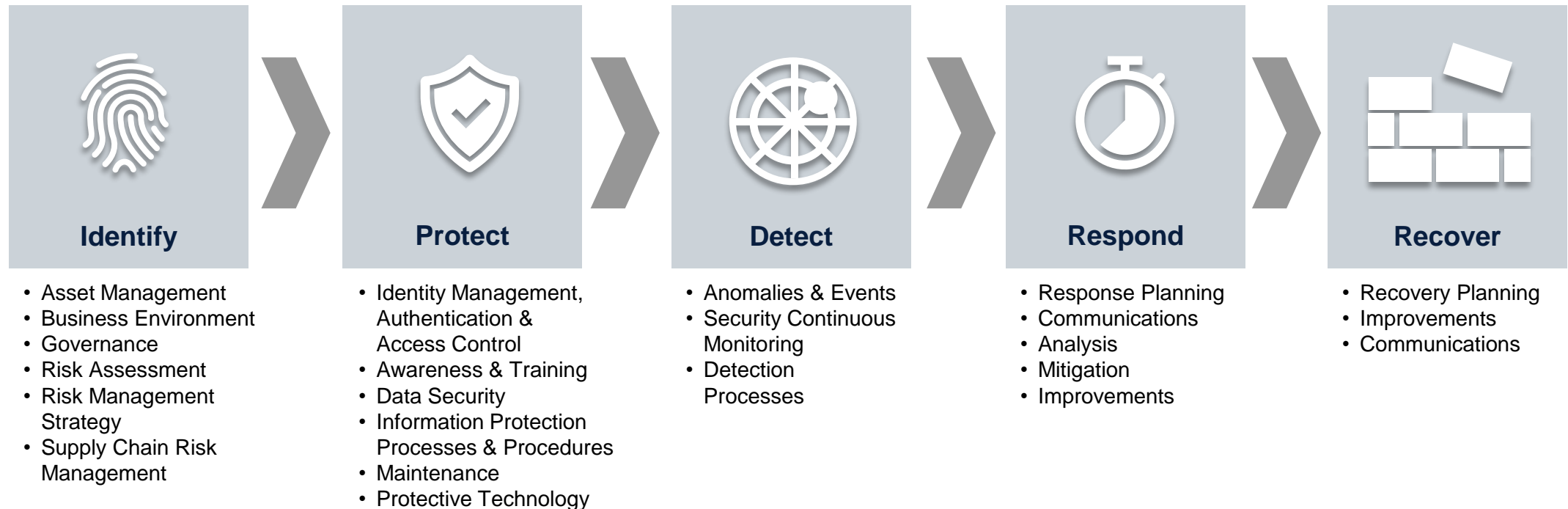
Fla. Sta. 282.3185(4)(1):

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)

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



Source: [NIST Cybersecurity Framework](#)

(T)

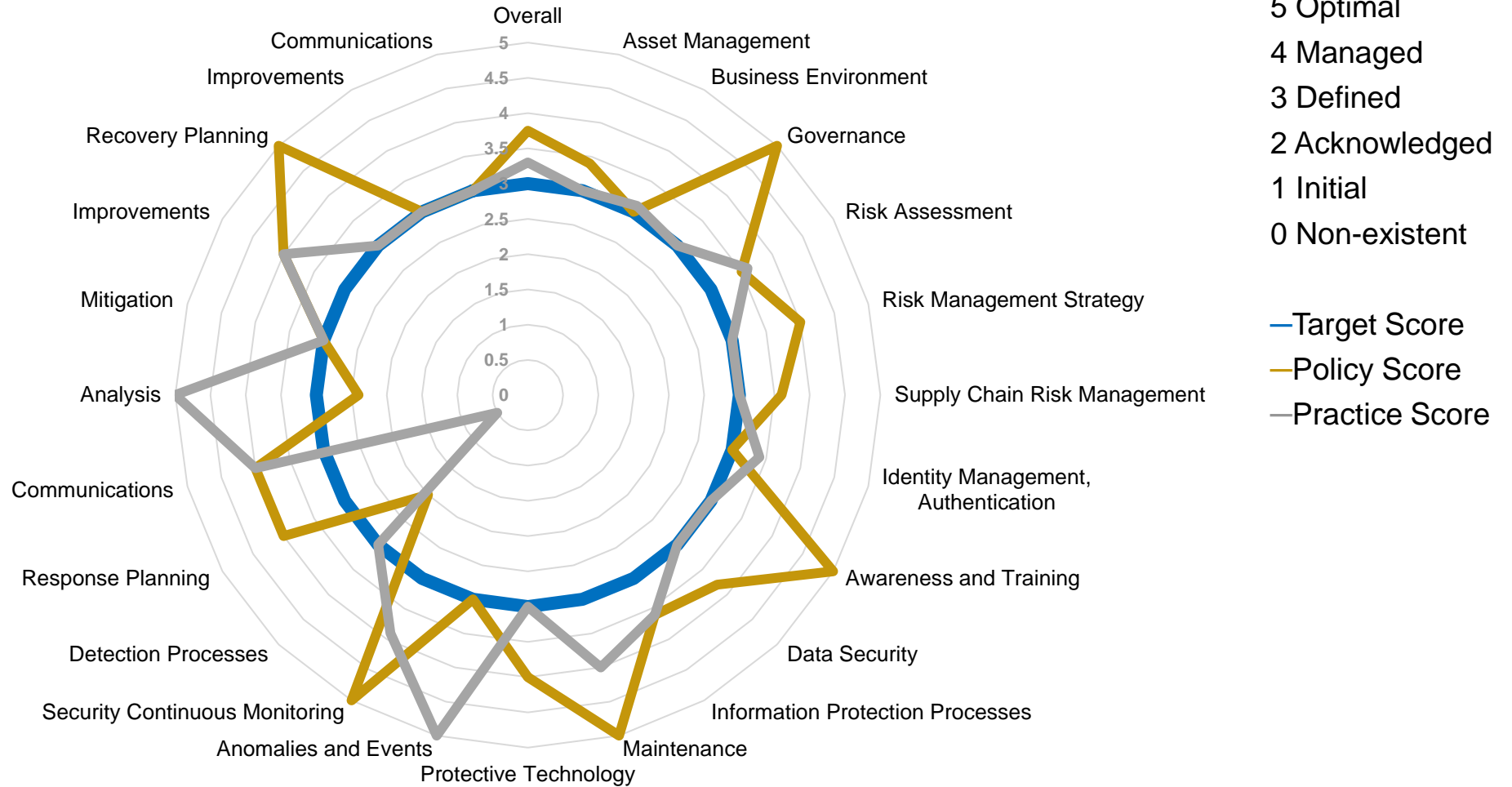
(S)

(P)

Maturity Assessment

Very difficult (but important) to perform!

Sample NIST Cyber Security Framework Maturity Levels



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

Question:

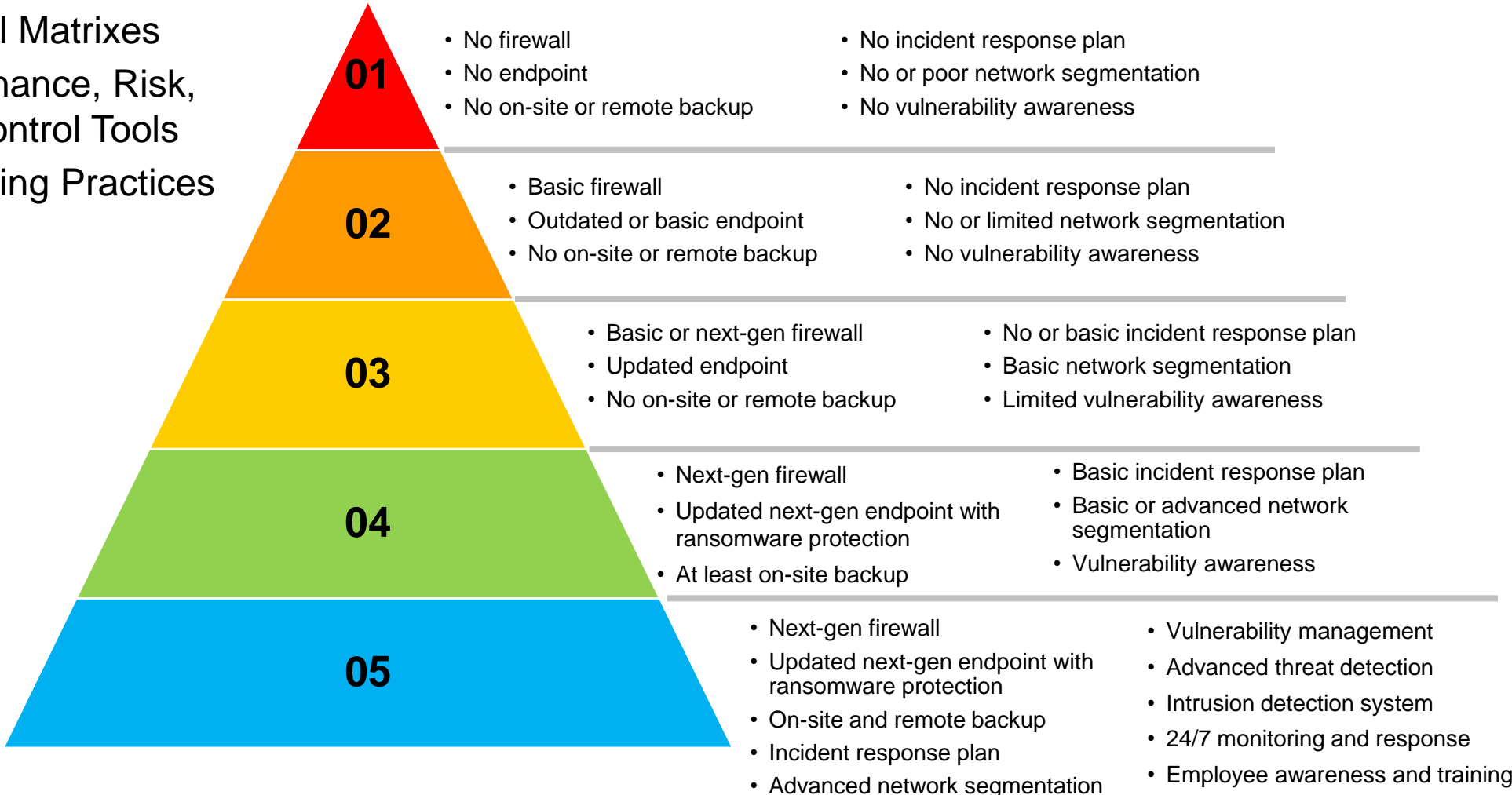
What is one of the key requirements of Florida Statute 282.3185?

- A. Conducting regular risk assessments
- B. Providing free public Wi-Fi
- C. Increasing tax revenue
- D. Enhancing employee productivity

Cybersecurity Risk Management (P)

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

Sample Cybersecurity Maturity Model



(P)



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

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!

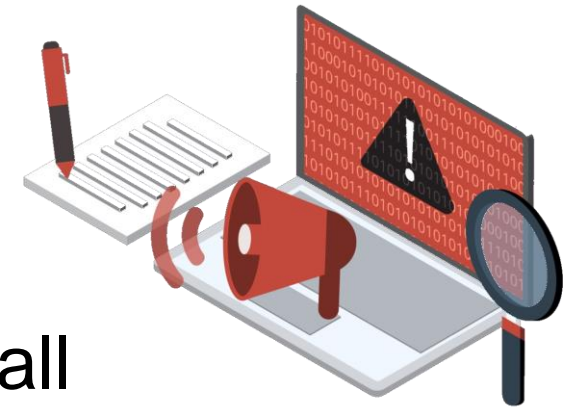
(T)

(S)

(P)

(O)

Reporting Requirements Florida

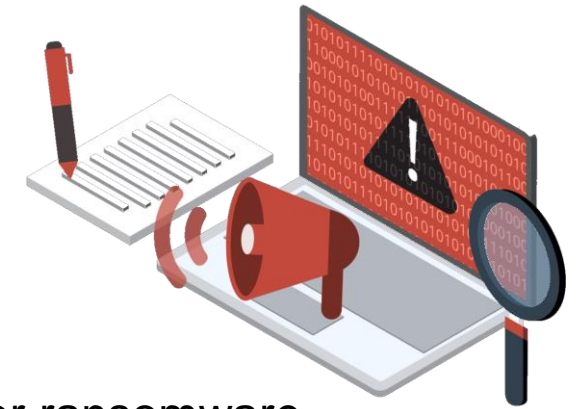


A state agency or local government shall report all **ransomware** incidents and any cybersecurity incident determined by the state agency to be of severity level 3, 4, or 5 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement as soon as possible but **no 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)

(P)

(O)

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**

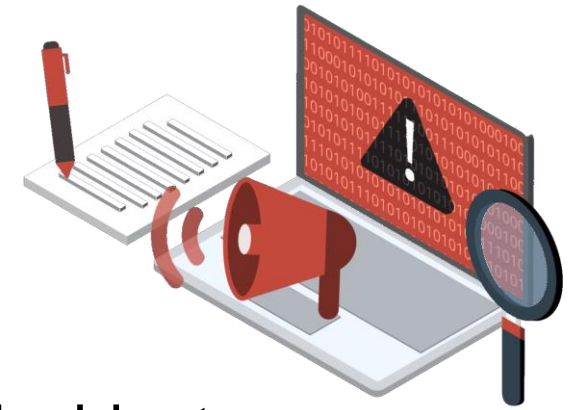
They also must add the following:

- 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.**

(P)

(O)

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)

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 Cyber Incidents In Florida

(T)

- 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

(P)



(O)

The Reality

- Attacks are more frequent and more sophisticated
- Organizations are struggling to manage their enterprise cybersecurity initiatives
- In many organizations **Cybersecurity is not a strategic priority**
- The urgency to prepare and invest in incident response usually occurs **only after an event with a significant impact**
- Qualified resources (**Cyber talent**) is becoming a **critical issue**
- Legal, compliance and security **complexities managing Third Party Vendors**
- Automated attacks require automated defenses (challenges identifying the right solutions)

(S)

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

Question:

What is the primary reason cybersecurity is crucial for government finance leaders?

- A. Protecting sensitive data
- B. Avoiding financial losses
- C. Ensuring public trust
- D. All of the above



Post Course Survey

FIU

Jack D. Gordon
Institute for Public Policy

Thank You!

**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

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

- 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 Best Practices for Smart Cities
Source: Cybersecurity-best-practices-for-smart-cities_508.pdf
- State 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.

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>
- Cybersecurity Best Practices for Smart Cities
Source [Cybersecurity-best-practices-for-smart-cities_508.pdf](#)
- State 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)