The JAMES MADISON INSTITUTE
Trusted Solutions for a Better Florida

ISSUE COMMENTARY / DECEMBER 2024

Protecting Paradise: Cybersecurity in the Sunshine State

Dr. Edward Longe *Director of the Center for Tech & Innovation, The James Madison Institute*

Executive Summary

Florida's cybersecurity landscape faces unprecedented challenges, as evidenced by several major breaches in 2024, including the theft of 20,000 sensitive files from the *Florida Department of Health* and a system-wide shutdown of North Miami's government operations. These incidents highlight a broader pattern of vulnerability: in 2023, Florida recorded over 41,000 cyber incidents resulting in losses of $874.7 million, ranking third nationally in both total incidents and financial impact.

The state's large elderly population makes it particularly attractive to cybercriminals. Currently home to 5.5 million residents over age 60—outnumbering the senior populations of 20 other states combined—Florida's elderly demographic is projected to reach 8.4 million by 2045. This is especially concerning as seniors are the primary targets of cybercrime, with the Federal Bureau of Investigation (FBI) reporting national losses exceeding $3.4 billion among this age group in 2023.

The consequences of these attacks extend far beyond immediate financial losses. For businesses, the average cyberattack costs $4.88 million, with 60% of small businesses forced to close within six months of an incident. Individual victims often suffer both financial devastation and significant emotional trauma.

To combat these threats, Florida must implement a comprehensive strategy that includes sustained investment in government cybersecurity infrastructure; development of a balanced, safe harbor program; integration of AI-driven threat detection; mandatory K-12 cybersecurity education; and targeted protection programs for elderly residents. Additionally, addressing the critical shortage of cybersecurity professionals—currently estimated at

500,000 nationwide—must be a priority. These measures require immediate legislative action and sustained investment to protect Florida's digital infrastructure and its most vulnerable residents.

The Issue: On June 26, 2024, the *Florida Department of Health* (FDOH) discovered a security breach in which international cybercriminals had stolen "20,000 department files that included some Floridians' most sensitive information: HIV test results, signed medical release forms, detailed insurance data, workers compensation records and COVID-19 diagnoses."[1] Just two months later, the *City of North Miami* was the victim of a cyberattack that forced the city to effectively close for over a week.[2] Government entities were not the only targets of cybercriminals in Florida. *National Public Data*, a Florida-based background check company, was the victim of a hack that saw almost every Social Security Number leaked on the dark web.[3] The leaks at FDOH, the *City of North Miami*, and *National Public Data* highlight that while the State of Florida has taken great strides over the past few years to enhance cyber resilience, the state and its residents remain vulnerable to nefarious actors and criminal networks seeking to acquire data.

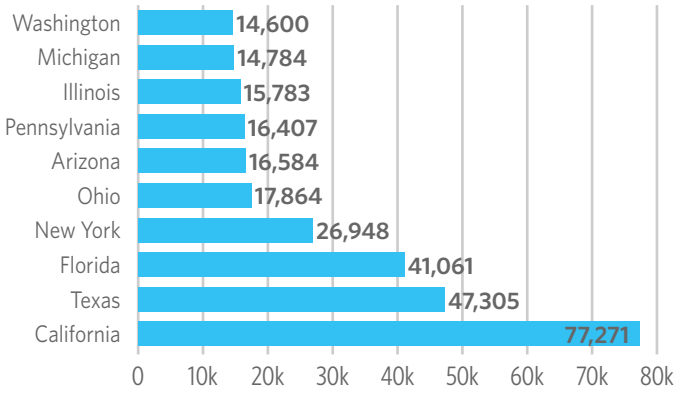
When initiating cyberattacks against public and private entities, criminal networks often look for data that could be held for ransom. In the case of the FDOH leak, *RansomHub,* the criminal network behind the attack, demanded money in return for the data. Once the deadline for payment passed, the data was leaked online, exposing the sensitive information of thousands of Floridians. Part of the reason governments, particularly state and municipal governments, are targeted, is because there is a perception that they are data rich, but cyber poor and thus vulnerable to attacks.[4]

Florida's Cyber-Insecurity: Unfortunately, the attacks against FDOH, the *City of North Miami*, and *National Public Data* were just three of the most publicized cyber incidents in Florida in 2024. In 2023, the FBI reported 41,061 cyber incidents in the state, approximately 112 incidents every day.[5] In terms of total incidents, Florida ranked third nationally for cyber incidents, behind Texas (47,305) and California (77,271).[6] As a result of these cyber incidents, which can range from phishing scams to malware attacks, the FBI estimates that Floridians lost $874.7 million in 2023 alone.[7] Florida again ranked third nationally behind Texas ($1,021.6 million) and California ($$2,159.5 million) for total losses from cyber incidents.[8]

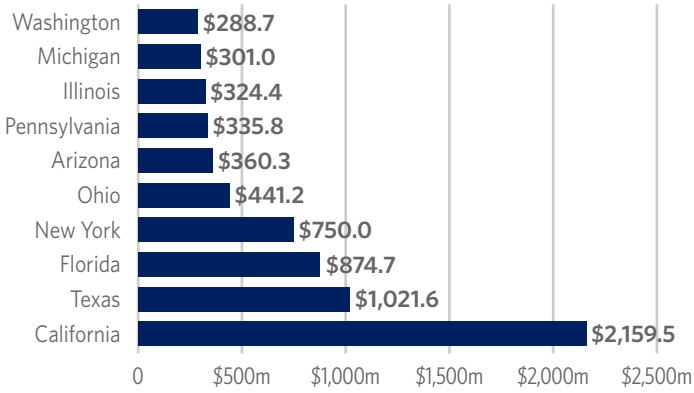
Florida is a particularly attractive state for cybercriminals given its large and growing elderly population. Currently, there are 5.5 million residents over the age of 60 in Florida, which outnumbers the senior "populations of 20 other states combined."[9] According to the *Florida Department of Elder Affairs*, "Florida is second only to California in the actual number of citizens age 60 and older."[10] By 2045, Florida's elderly population is expected to reach 8.4 million, comprising 30 percent of the state's population.[11]

Florida's growing elderly population is especially concerning for cyber professionals because they are the principal targets of cybercriminals. According to the FBI, Americans over the age of 60 reported the most cyber incidents in 2023, with losses totaling over $3.4 billion for American seniors.[12] They are generally targeted because of a perception among criminal networks, especially those abroad, that senior citizens "have ample retirement savings sitting in their bank account" as well as "cognitive issues that can make them prone to exploitation."[13] Further complicating matters is the fact that many senior Americans "live alone, with no one to help manage their money."[14] As Florida's elderly population grows, the state will increasingly become a ripe target for cybercriminals.

2023 - Top 10 States by Number of Complaints



2023 - Top 10 States by Loss (In Millions)



Source: FBI Internet Crime Report, 2023

Impact on Floridians: For businesses falling victim to a cyberattack, the results can be devastating. According to the *Identity Theft Resource Center,* 73% of small businesses were targets of cyberattacks in 2023, with each incident costing an average of $4.88 million.[15] Part of this cost is because businesses must close imme-

diately after the attack, data recovery is often expensive, and companies that fall victim are often subject to lawsuits and regulatory fines. It's also estimated that 60% of small businesses will close after falling victim to a cyberattack due to catastrophic reputational damage.[16] Such closures can be crippling for local economies as recovering from cyberattacks prevents businesses from investing in scaling operations and hiring new staff and business closures lead to job losses and individuals moving away from their communities.

For individuals, falling victim to cybercrime can be equally devastating. Beyond the financial loss, which can run into thousands of dollars, victims also report significant trauma, including "fear, anxiety, betrayal, and emotional distress."[17]

Legislative Responses

In response to the growing threat posed by cybercriminals, states have taken steps to incentivize good cybersecurity practices. Utah and Tennessee, for example, both created a cybersecurity safe harbor for entities that fall victim to cyberattacks despite largely complying with industry standards.[18] The logic behind both measures is that the safe harbor, which provides immunity from litigation, will incentivize everyone to enhance their cybersecurity program and provide better protections. During the 2024 legislative session, the Florida legislature passed a bill to create a Cybersecurity safe harbor, however, the measure was vetoed by Governor DeSantis who feared the measure would incentivize "doing the minimum when protecting consumer data."[19] Governor DeSantis did, however, invite "all interested parties" to "review alternatives to the bill that provide a level of liability protection" while also ensuring consumer data remains secure.[20]

Cybersecurity is also dependent on investment from the legislature, particularly when enhancing the cybersecurity of state and municipal governments. As part of the 2024 budget, Florida's legislature appropriated $40 million in competitive grants to provide "local governments with software, services, and solutions that enhance local governments' cybersecurity posture to protect their infrastructure and Floridians' data."[21] The $40 million grant follows significant investments from the legislature in previous years. Without these investments, municipal governments and state agencies are not able to update their systems to provide greater cyber protections which in turn creates unnecessary vulnerabilities.

Policy Principles

Continue Investments in Cybersecurity: The legislature must continue making investments to ensure Florida becomes a leader in national cybersecurity education. These investments must be targeted toward educating government employees to address current and emerging cyber threats while updating government technology.

Cybersecurity Safe Harbor: The legislature and executive branch must come to a compromise on a cybersecurity safe harbor that provides liability protection for organizations complying with accepted industry cybersecurity practices.

Embrace the use of AI: Artificial Intelligence has the capability to detect cybersecurity threats as they happen and predict and respond to them. Government agencies should embrace the use of AI as part of their cyber defense program to ensure they are capable of responding to increasingly complex threats earlier.

Educate Florida's Elderly: As Florida's elderly population continues to grow, the state will become increasingly attractive to foreign and domestic cyber criminals. Lawmakers should prioritize educating Florida's elderly population about current and emerging threats and what they can do to protect themselves from cybercrime.

Close the Workforce Gap: In June 2024, Homeland Security Chairman Mark E. Green reported to Congress that America is short 500,000 cybersecurity professionals, a shortage that is estimated to grow in the coming years.[22] Such a significant workforce shortage creates unnecessary cyber vulnerabilities for both public and private entities. In fact, the shortage of workers has become so acute that the *National Institute of Standards and Technology* estimates that "By 2025, lack of talent or human failure will be responsible for over half of significant cybersecurity incidents."[23] Florida must work in conjunction with the private sector and educational institutions to invest in training programs that will close the workforce gap.

Make Cybersecurity Part of the K-12 Curriculum: Today's students need comprehensive cybersecurity education that grows with them throughout their academic journey. Public schools have a responsibility to educate their students on good cybersecurity practices to prevent students from falling victim to cybercrime. Currently, cybersecurity is not mandated as part of the K-12 curriculum in Florida, however, CyberFlorida's Operation K12 is active in 45 districts across the state,[24] and the *Florida Department of Education* offers an Applied Cybersecurity Program.[25] The legislature should mandate these programs.

References

1 Lawrence Mower, "Health department now notifying Floridians whose information was stolen, leaked," *Tampa Bay Times,* August 21, 2024. Available Online: https://www.tampabay.com/news/florida-politics/2024/08/21/florida-hacking-health-records-cyberattack-desantis-ladapo/

2 Joanne Haner, "North Miami Works to Restore Services After Cyber Attack," *Government Technology,* August 16, 2024. Available Online: https://www.govtech.com/security/north-miami-works-to-restore-services-after-cyber-attack

3 Sean Michael Kerner, "Social Security Number Data Breach: What You Need To Know," *TechTarget*, August 19, 2024. Available Online: https://www.techtarget.com/whatis/feature/Social-Security-number-data-breach-What-you-need-to-know#:~:text=National%20Public%20Data%20disclosed%20a,and%20current%20and%20past%20addresses.

4 Clayton Romans, "The Top Four Things Tech Manufacturers can do to Bolster the Cybersecurity of Target-Rich, Cyber-Poor Organizations," *Cybersecurity and Infrastructure Security Agency*, May 9, 2024. Available Online: https://www.cisa.gov/news-events/news/top-four-things-tech-manufacturers-can-do-bolster-cybersecurity-target-rich-cyber-poor-organizations

5 *Federal Bureau of Investigation*," Internet Crime Report, 2023." Avaliable Online: https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

6 Ibid.

7 Ibid.

8 Ibid.

9 *Florida Department of Elder Affairs, "Florida State Plan on Aging, 2022-20225."* Available Online: https://elderaffairs.org/wp-content/uploads/FINAL-Florida-State-Plan-on-Aging-2022-2025-10182021.pdf .

10 Ibid.

11 Ibid.

12 *Federal Bureau of Investigation*," Internet Crime Report, 2023."

13 *National Council on Aging*, "What Are the Top Online Scams Targeting Older Adults?," July 17, 2024. Avaliable Online: https://www.ncoa.org/article/what-are-the-top-online-scams-targeting-older-adults/

14 Ibid.

15 *Identity Theft Resource Center, "2023 Business Impact Report."* Available Online: https://www.idtheftcenter.org/wp-content/uploads/2023/10/ITRC_2023-Business-Impact-Report_V2.1-3.pdf; IBM, "Cost of Data Breach Report 2024."

16 Robert Johnson, III"60 Percent Of Small Companies Close Within 6 Months Of Being Hacked," *Cybersecurity Magazine, Jan. 2, 2019* https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

17 Esteban Borges, "Types of Cyber Crime: A Guide to Prevention & Impact," *Recorded Future, June 26, 2024.* Available Online: https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/types-of-cybercrime

18 Utah Cybersecurity Affirmative Defense Act. Available Online: https://le.utah.gov/xcode/Title78B/Chapter4/C78B-4-P7_2021050520210505.pdf; Tennessee Code Annotated, Title 29, Chapter 34, Part 2. Available Online: https://www.capitol.tn.gov/Bills/113/Bill/SB2018.pdf

19 Governor Ron DeSantis, "Veto Message: HB473." June 26, 2024. Available Online: https://www.flgov.com/wp-content/uploads/2024/06/Veto-Letter_HB-473.pdf

20 Ibid.

21 *Florida Digital Service, "Florida Local Government Grant,"* Available Online: https://cybergrants.fl.gov/

22 House Committee on Homeland Security, Hearing Announcement: Finding 500,000. Available Online: https://homeland.house.gov/2024/06/21/media-advisory-chairman-green-announces-hearing-on-americas-cyber-workforce-shortage-amid-rising-threats/

23 *National Institute of Standards and Technology,* "Cybersecurity Workforce Demand." Available Online: https://www.nist.gov/system/files/documents/2023/06/05/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf

24 CyberFlorida, "Operation K12." Available Online: https://cyberflorida.org/opk12/

25 *Florida Department of Education, "Information Technology."* Available Online: https://www.fldoe.org/academics/career-adult-edu/career-tech-edu/curriculum-frameworks/2021-22-frameworks/info-technology.stml

The James Madison Institute
The Columns
100 North Duval Street
Tallahassee, FL 32301

850.386.3131

www.jamesmadison.org