CYBERSECURITY

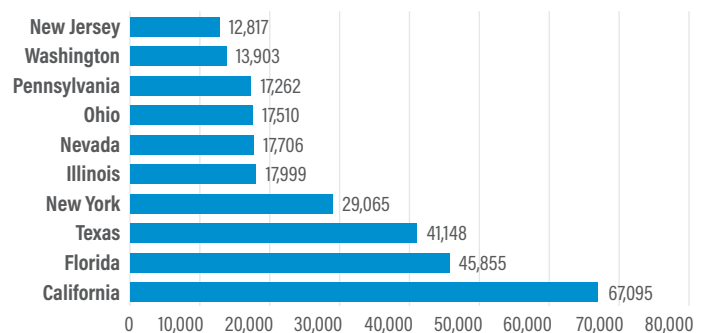*The* JAMES
MADISON
INSTITUTE
Trusted Solutions for a Better Florida

⊙ The Issue: On February 2nd, 2023, Tallahassee Memorial Healthcare experienced an "IT Security Incident"[1] that forced it to turn patients away and return to paper charts and admission forms. The incident, which is widely believed to have been a ransomware attack, further highlighted Florida's cyber vulnerabilities and the growing threat posed by cybercriminals, despite being widely regarded as one of the most digitally secure states in America.
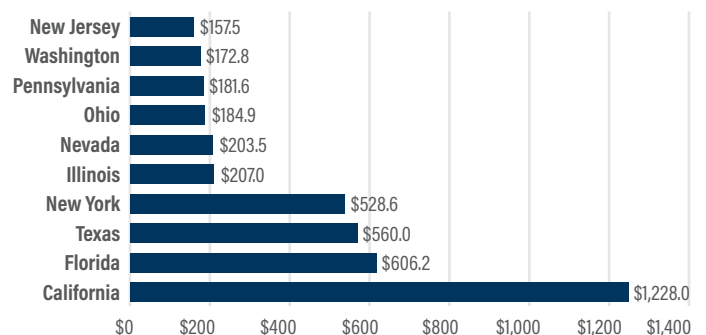
While the hack against Tallahassee Memorial Healthcare was the most widely publicized incident, the Federal Bureau of Investigation (FBI) reported over 2,300 daily incidents in 2021.[2] When initiating cyberattacks against public and private entities, criminal networks are often looking for money, financial information, and medical information that can be held for ransom. For businesses, these cyberattacks can have significant reputational and financial ramifications, costing them an estimated $200,000.[3] It's estimated that 60% of small businesses will close after falling victim to a cyber attack.[4]

⊙ Florida's Cyber-insecurity: Given its booming population and economy, it's unsurprising that Floridians are increasingly targeted by cybercriminals. In 2021, the FBI reported that 45,855 Floridians had fallen victim to cybercrime with total losses estimated to be $528,573,929.[5] In terms of total victims, Florida is second only to California and fourth nationally in terms of total losses.[6]

2021 - Top 10 States by Number of Victims

State	Number of Victims
New Jersey	12,817
Washington	13,903
Pennsylvania	17,262
Ohio	17,510
Nevada	17,706
Illinois	17,999
New York	29,065
Texas	41,148
Florida	45,855
California	67,095

2021 - Top 10 States by Victim Loss in $Millions

State	Victim Loss ($Millions)
New Jersey	$157.5
Washington	$172.8
Pennsylvania	$181.6
Ohio	$184.9
Nevada	$203.5
Illinois	$207.0
New York	$528.6
Texas	$560.0
Florida	$606.2
California	$1,228.0

Source: FBI Internet Crime Report, 2021

LEGISLATIVE RESPONSES

In September 2022, Governor Ron DeSantis issued an executive order that prohibited state entities from purchasing or using technology from countries like Cuba, Russia, Iran, North Korea, Syria, Venezuela, and China.[7] The justification for such an executive order was that these nations are hostile to the United States and could use this technology to disrupt critical infrastructure.

DeSantis' administration has also provided significant financial investment. Most recently, Governor DeSantis proposed $149 million as part of his Framework for Freedom Budget to provide "both state and local governments…the tools necessary to protect critical public resources and sensitive information."[8] Additionally, his administration provided $15.6 million to expand cybersecurity training programs,[9] and $20 million which will be "directed toward the University of South Florida, which will coordinate three regional partnerships to develop workforce education clusters in cybersecurity or cyber-related disciplines for middle-school, high-school, and college students."[10]

The state legislature has also prioritized cybersecurity. In June 2022, the legislature enacted HB 7055 and the State Cybersecurity Act, which required state and municipal agencies to report certain cyberattacks within 48 hours, prohibited them from paying any ransom demands, and also established cybersecurity training requirements for state and municipal employees. While this was a step in the right direction, the legislature must do more to strengthen cybersecurity legislation in Florida.

POLICY RECOMMENDATIONS

1. Invest in cybersecurity training programs.
The legislature must continue making investments to ensure Florida becomes a leader in national cybersecurity education. These investments must also be targeted toward state and municipal employees.

2. Prevent state agencies and municipalities from using technology made in hostile countries
The legislature should pass legislation that would prohibit government agencies that hold sensitive information of Florida residents from contracting with companies domiciled in adversarial nations. Such rules would make it considerably harder for foreign nations to launch cyber attacks against Florida.

3. Provide incentives for cyberattack reporting.
Not every cyberattack is reported to state or federal authorities, even when required by law. This lack of reporting makes it difficult to grasp the full scale of the cybersecurity problem. The legislature must create a series of incentives, such as safe harbor, to incentivize companies to invest in cybersecurity programs and report incidents.

4. Make cybersecurity part of the K-12 curriculum.
As children's lives increasingly take place online, schools have a responsibility to provide training on good cybersecurity practices to prevent students from falling victim to cybercrime.

ENDNOTES

1   Tallahassee Memorial Healthcare, "Tallahassee Memorial Managing IT Security Issue," February 3, 2023.
    Available Online: https://www.tmh.org/news/2023/tallahassee-memorial-managing-it-security-issue
2   Federal Bureau of Investigation," Internet Crime Report, 2021."
    Available Online: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
3   Hiscox, "Hiscox Cyber Rediness Report, 2019." Available Online: https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf
4   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/
5   Federal Bureau of Investigation," Internet Crime Report, 2021."
6   Ibid.
7   State of Florida, Office of the Governor, Executive Order 22-216 "Strengthening Florida Cybersecurity Against Foreign Adversaries." Sep 22, 2022,
    Available Online: "https://www.flgov.com/wp-content/uploads/2022/09/Executive-Order-22-216.pdf
8   Governor Ron DeSantis, "Framework for Freedom Budget, Fiscal Year 2023-2024."
    Available Online: http://www.floridaleadsbudget.com/PDFLoader.htm?file=GeneralGovernment.pdf
9   Governor Ron DeSantis, "Governor Ron DeSantis Awards $15.6 Million to Expand Access to Cybersecurity and IT Training," June 29, 2022.
    Available Online: https://www.flgov.com/2022/06/29/governor-ron-desantis-awards-15-6-million-to-expand-access-to-cybersecurity-and-it-training/
10 Governor Ron DeSantis, "Governor Ron DeSantis Announces $20 Million to Create Cybersecurity and Information Technology Workforce Education Opportuni-
    ties," March 2, 2022. Available Online: https://www.flgov.com/2022/03/02/governor-ron-desantis-announces-20-million-to-create-cybersecurity-and-infor-
    mation-technology-workforce-education-opportunities/