Florida Critical Infrastructure Cybersecurity Intelligence Assessment

Dr. Steve Gary, CISSP
School of Information
University of South Florida

Dr. Randy Borum, ABPP
School of Information
University of South Florida

RJ Burney
Overwatch OT

June 2023

Executive Summary

The cybersecurity of Florida's critical infrastructure (CI) is a prime concern. We assess the current, overall cyber threat risk to Florida's CI as MODERATE (*on a scale of low, moderate, and high). China, Russia, North Korea, and Iran currently pose the most significant threat among the nation-state cyber threat actors. Russia's cyber-attacks often aim to influence foreign citizens and governments and undermine democratic institutions. Ransomware and custom malware are two of their common tactics. They have also shown a sustained interest in underwater cables and industrial control systems. China and Iran (often as a Chinese Proxy) have both been active in stealing research and development (R&D) and intellectual property (IP) to shorten their R&D timelines and to develop products to improve their economy and enhance or accelerate their military capabilities. China has also significantly compromised supply chains to bolster these aspirations. Florida is a prime target for this kind of theft because of the number of research universities and technology companies conducting R&D and relying on IP. North Korea's major attacks have been motivated primarily by financial gain, often targeting financial institutions, banking systems, blockchain companies, and cryptocurrency exchanges (stealing over $2.5B). Iran's most robust advanced persistent threat (APT) groups have shown a particular interest in the aviation, energy (targeting industrial control systems), and petrochemical industries. These nation-state cyber activities will continue to pose threats to Florida's CI for the foreseeable future, and once coupled with generative artificial intelligence (AI) these threats will increase.

Florida's CI, businesses, and citizens continue to be attractive targets for cybercriminals who often use ransomware, theft, and scams for financial gain. According to the FBI's 2022 Internet Crime Report, Florida ranks at the top (second only to California) nationally for the most victims and dollars lost to cybercrime. Phishing attacks, personal data breaches, theft through non-payment/non-delivery, and investment fraud are some of the most significant cybercrime threats. Insider threats also continue to pose a persistent risk to CI in Florida and have grown to include threat actors being inserted or hired into these organizations. Ransomware attacks (primarily through phishing) have accelerated and expanded in several CI sectors, especially healthcare, critical manufacturing, government facilities and information technology (IT). Bottom line,

cyber threat actors are constantly attacking and probing CI networks for access points and vulnerabilities.

The cyber threat assessment report recommends that Florida CI owners and operators prioritize cyber intelligence and maintain a high degree of situational awareness to understand the capabilities, intentions, and activities of adversaries and threat surfaces within their CI sectors and subsectors. Cyber intelligence should guide their cybersecurity posture and decision making to better anticipate threats. Some recommended cyber threat prevention and mitigation techniques include cybersecurity awareness training for employees, operators, and end-users; enforced multi-factor authentication; immediate and continuous patching of known vulnerabilities; securing systems' remote access;[1] architectural resilience; and active monitoring of internal and external IT and operational technology (OT) networks for security risks.

[1] Adams (2022). *Remote network access: Understanding remote network access protocols and types*. Article: Business Tech Weekly. Available at: https://www.businesstechweekly.com/cybersecurity/network-security/remote-network-access/

Cyber Threat Actors

Cyber threats are sometimes cursorily viewed as lines of code and malicious programs and tactics. But the adversarial actors behind the keyboard are the root cause of the threat. According to a Mandiant survey, "96% of security decision makers believe it is important to understand which cyber threat actors could be targeting their organization."[2] In cybersecurity, a range of diverse cyber threat actors (CTAs)—often with different methods (tactics, techniques, and procedures or TTPs) and motives—can threaten critical infrastructure (CI).[3]

Nation-state

International norms have generally prohibited nation-states from attacking critical infrastructure.[4] However, because disrupting, controlling, destroying, or stealing from CI can produce such profound effects, such attacks are not uncommon. There is evidence that the average number of cyber-attacks against CI jumped 62% between 2022 and 2023.[5] The U.S.'s 2023 *National Cybersecurity Strategy* calls out four specific nation-states whose CTAs are actively engaged in malicious cyber activity against U.S. interests: China, Russia, North Korea, and Iran. Collectively, these four countries account for more than 75% of all state-sponsored cyber-attacks worldwide since 2005[6] and are likely to pose the greatest cyber threat to CI in the U.S.:

> *The governments of China, Russia, Iran, North Korea, and other autocratic states with revisionist intent are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms. Their reckless disregard for the rule of law and human rights in cyberspace is threatening U.S. national security and economic prosperity.*[7]

China

China (officially the People's Republic of China or PRC) currently maintains some of the highest-level cyber capabilities (in sophistication and volume) among the U.S.'s foreign nation-state adversaries/competitors. They have also demonstrated their intent to use those capabilities against U.S. security interests, particularly in the economic sphere. The U.S. Intelligence

[2] Mandiant (2023). *Global Perspectives on Threat Intelligence*. Report: Mandiant.

[3] Lanz, Z. (2022). Cybersecurity Risk in U.S. Critical Infrastructure: An Analysis of Publicly Available U.S. Government Alerts and Advisories. *International Journal of Cybersecurity Intelligence & Cybercrime: 5(1)*, 43-70. Available at: https://vc.bridgew.edu/ijcic/vol5/iss1/4

[4] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/70/174.

[5] Bridewell (2023). Cyber Security in Critical National Infrastructure Organisations: 2023. Research Report: Bridewell.

[6] Council on Foreign Relations (2023). *Cyber Operations Tracker*. Report: Digital and Cyberspace Policy Program, Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/

[7] The White House (2023). *National Cybersecurity Strategy*. Report: The White House, Washington, DC, p. 3.

Community (IC) believes that China may represent the “broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks” and that they are capable of disrupting critical infrastructure (CI) services within the United States.[8]

China’s Advanced Persistent Threat (APT) groups are numerous (over 30) and diverse (government, military, and civilian), with many having specialized, focused, and dedicated missions. In June 2023, the NSA, CISA, FBI and all of Five Eyes (FVEY) partner nations issued a Joint Cybersecurity Advisory concerning a CTA associated with China known as “Volt Typhoon.” According to the Advisory “Private sector partners have identified that this activity affects networks across U.S. critical infrastructure sectors, and the authoring agencies believe the actor could apply the same techniques against these and other sectors worldwide.” Volt Typhoon often evades detection and avoids triggering intrusion alerts by using built-in network administration tools to blend in with normal Windows system and network activities. [9] Those tactics are part of a larger trend of Chinese activity identified by Mandiant where CTAs, rather than directly infiltrating systems behind the firewall, are targeting the firewall itself or devices on the edges of the network (e.g., sensors, controllers, Internet of Things) that are less likely to carry antivirus or end-point detection software.[10]

Three additional areas of Chinese cyber activity are particularly concerning. First, China continues to steal research and development (R&D) and intellectual property (IP) to shorten their R&D timelines and to develop products to improve their economy and enhance or accelerate their military capabilities. Florida’s research universities are a primary R&D target. Second, China seeks to infiltrate networks and U.S.-based information systems not only to steal R&D and IP, but also to surveil and collect information about U.S. CI. In addition to direct cyber-attacks, China is building serious vulnerabilities into technology and services (to be deployed in the U.S.) that may include malicious code designed to illegally gather, disrupt, or destroy sensitive or proprietary information. Third, China is seeking to influence U.S. companies –both directly and indirectly though vendors in the supply chain—by funding them, purchasing or securing ownership interest in them, and placing personnel in key decision-making positions within these companies.

Looking forward, two additional cautions—one national and one specific to Florida—are worth noting. The national caution pertains to assessments from the U.S. IC and within the private sector suggesting that China’s threat to CI—particularly in the transportation, energy, and water sectors—is likely to increase if PRC mounts military operations to invade Taiwan or otherwise anticipate significant, imminent conflict with the U.S. The threat of Chinese incursion in Taiwan is neither remote nor speculative. It is clear that Xi has already directed his military to prepare

[8] Office of the Director of National Intelligence (February 6, 2023*). Annual Threat Assessment of the U.S. Intelligence Community*. Report: Office of the Director of National Intelligence.

[9] Joint Cybersecurity Advisory (June, 2023). People’s Republic of China State Sponsored Cyber Actor Living Off the Land to Evade Detection. Advisory: DoD. Available at: https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

[10] McMillan, R. & Volz, D. (March 16, 2023). Wave of Stealthy China Cyberattacks Hits U.S., Private Networks, Google Says. Article: WSJ. Available at: https://www.wsj.com/articles/wave-of-stealthy-china-cyberattacks-hits-u-s-private-networks-google-says-2f98eaed

itself for such action and, while there is not consensus on their anticipated timeline, some estimates put it as early as 2025.[11]

A statewide caution is noted because over the past year, and particularly in Spring 2023, the State of Florida has enacted Executive policies and passed legislation that may have economic consequences for the PRC, including laws that limit acquisition and use of Chinese technologies and restrict Chinese Nationals from buying property in Florida. While China has historically sought to "exploit U.S. subnational relationships to influence U.S. policies and advance PRC geopolitical interests,"[12] most known efforts to date have involved political manipulation, coercion and deceptive incentives rather than retributive or “protest” cyber-attacks. It is certainly possible, however, that the recent round of rhetoric and legislation designed “to counteract the malign influence of the Chinese Communist Party in the state of Florida”[13] will motivate PRC/CCP-affiliated CTAs to amplify their interest in Florida—particularly through state and local governments—as a potential target.

Finally, other statewide areas of concern regarding China are Florida’s ports, e.g., cyberspying via Chinese-made cranes;[14] military installations, including the major commands, i.e., U.S. Special Operations Command, U.S. Central Command, and U.S. Southern Command; and its large concentration of financial institutions and crypto firms, including those in Miami’s “crypto beach.” Bottom line, Florida’s growing economy (fourth largest in the U.S.) and the recent bills passed by the Governor to target Chinese influence in Florida will likely provoke more Chinese cyber actions.[15]

Russia

Russia has a broad and robust capability for engaging in malicious cyber activity. They have also demonstrated their intent to use those capabilities against U.S. security interests and particularly to target U.S. critical infrastructure (CI). In May 2023, the U.S. Department of Justice charged a Russian national who “allegedly used multiple ransomware variants to attack critical

[11] Hearing to Receive Testimony on Worldwide Threats, 118th Congress 85 (May 4, 2023) (testimony of Lt. Gen. Scott Berrier, Director, Defense Intelligence Agency).

[12] NCTSC (July, 2022). *Protecting Government and Business Leaders at the U.S. State and Local Level from People’s Republic of China (PRC) Influence Operations*. National Counterintelligence and Security Center. https://www.odni.gov/files/NCSC/documents/SafeguardingOurFuture/PRC_Subnational_Influence-06-July-2022.pdf

[13] Office of Governor Ron DeSantis. (May 8, 2023). *Governor Ron DeSantis Cracks Down on Communist China*. [Press release]. https://www.flgov.com/2023/05/08/governor-ron-desantis-cracks-down-on-communist-china/

[14] Lyons (2023). *Lawmakers fear cyberspying from Chinese-made cranes in South Florida ports*. Article: South Florida Sun Sentinel. Available at: https://www.sun-sentinel.com/2023/04/04/lawmakers-fear-cyberspying-from-chinese-made-cranes-in-south-florida-ports/

[15] Tuner (2023). *DeSantis approves a trio of bills targeting Chinese influence in Florida*. Article: WUSF Public Media. Available at: https://wusfnews.wusf.usf.edu/politics-issues/2023-05-09/desantis-approves-bills-targeting-chinese-influence-florida

infrastructure around the world, including hospitals, government agencies, and victims in other sectors."[16]

Russia's malicious cyber actors have a range of motives, from criminal groups working primarily for financial gain to military and security-based groups attempting to engage in espionage, influence U.S citizens, amplify societal discord, and undermine America's democratic institutions. In the wake of Russia's invasion of Ukraine, cross-over activity has accelerated where some cybercrime collectives—in solidarity with the Russian Government—have increasingly engaged in disruptive attacks to support the military offensive.[17] While Russia over the past year has exerted intense cyber activity against Ukraine, they have also used those malicious capabilities to push back against the resulting severe economic sanctions imposed on them by the U.S. and its allies. They have proven their ability to disrupt CI in recent attacks on Georgia, Estonia, Crimea, and Ukraine.

Russia's well-established APTs—APT 28 and APT 29—are probably best-known in the U.S. for hacking the Democratic National Committee (DNC) during the 2016 elections. APT 28 (sometimes referred to by names such as Fancy Bear and Sofacy)—well-known for their spear-phishing attacks—is almost certainly associated with Russian military intelligence (GRU). APT 29 (sometimes referred to by names such as Cozy Bear and The Dukes)—with its sophisticated use of custom malware—has been similarly linked to Russia's Foreign Intelligence Service (SVR). The U.S. Intelligence Community believes that "Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions….and is particularly focused on improving its ability to target CI, including underwater cables and industrial control systems."[18] Bottom line, Russia has tested and proven its cyber-attack capabilities on CI.

North Korea

North Korea—formally known as the Democratic People's Republic of Korea (DPRK)—has continued to develop and improve their cyber capabilities over time. While not reaching the scale or sophistication of China or Russia, those capabilities are significant. Most of DPRK's major attacks have been motivated primarily by financial gain, often targeting financial institutions, banking systems, blockchain companies, and cryptocurrency exchanges (stealing over $2.5B). Because Florida has a robust international presence in the Financial Services industry and houses America's third-largest cluster of insurance and banking companies, it could be an attractive

[16] U.S. Department of Justice, Office of Public Affairs (May 16, 2023*). Russian National Charged with Ransomware Attacks Against Critical Infrastructure*. Article: Justice News, U.S. Department of Justice, Office of Public Affairs.

[17] Critical Infrastructure and Security Agency (2022). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, Cybersecurity Advisory, Alert Code AA22-110A. Advisory: Critical Infrastructure and Security Agency.

[18] Office of the Director of National Intelligence (February 6, 2023*). Annual Threat Assessment of the U.S. Intelligence Community*. Report: Office of the Director of National Intelligence.

target for attacks on that critical infrastructure (CI) sector.[19] Florida has more than 135,000 financial and professional services firms with more than 900,000 professionals working in the state's finance, insurance, and professional services industries.

DPRK has reportedly placed, through deceptive means, thousands of "highly skilled" illicit IT workers in U.S. tech companies who send 90% of their earnings back to the regime. The revenue is heavily used to fund their nuclear weapons development and ballistic missile programs. According to a May 2023 advisory from the U.S. Department of treasury, "although these workers normally engage in IT work distinct from malicious cyber activity, we have also seen instances in which DPRK IT workers have provided some support to the DPRK's malicious cyber program through privileged access to virtual currency firms."[20] North Korea has also maliciously deployed their capabilities for political purposes to disrupt adversaries and competitors. The 2014 attack on Sony—while causing significant financial damage to the company—was likely an act of retaliation for creating a movie that parodied the country's leader in a way they perceived to be offensive. Many of North Korea's most sophisticated CTAs, including the group known as Lazarus or Hidden Cobra, are believed to be based in the Reconnaissance General Bureau (RGB), DPRK's foreign intelligence service. They have reportedly made numerous attempts to intrude into energy utilities (including those in the U.S.) and control systems, seeking in part to steal R&D and IP. Bottom line, in addition to financially motivated events, North Korea has used their cyber capabilities as a way to project power and they continue to pose a significant threat in the cyber domain to CI in the U.S.

Iran

Iran has invested heavily in building its offensive and malicious cyber capabilities. With extensive state-backing, those capabilities are mature, adaptive, agile, and persistent. Countering those efforts is like trying to hit a moving target. Tehran's cyber activities are primarily driven by political (domestic and foreign) and strategic motives rather than financial gain and are known to have targeted critical infrastructure (CI). For years, they have been known to target dozens of U.S. universities and government agencies. In September 2022, the U.S. Department of Justice charged three Iranian Nationals with computer intrusion (with data exfiltration) and ransomware attacks against multiple CI sectors, including health care centers, transportation services, and utility providers.

The concentration of major military installations in Florida, particularly U.S. Central Command and U.S. Special Operations Command in Tampa, may make the state particularly attractive to Iranian attackers with political/strategic motives. Iran's use of cyber-attacks against larger, better-resourced nations harmonizes with its more general leveraging of asymmetric strategy and tactics.

[19] Enterprise Florida (2023). *Financial and Professional Services*. Website: Enterprise Florida. Available at: https://www.enterpriseflorida.com/industries/financial-professional-services/

[20] U.S. Department of Treasury (May 23, 2023). Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities. U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). Available at: https://home.treasury.gov/news/press-releases/jy1498

The Islamic Revolutionary Guard Corps (IRGC) appears to coordinate most of Iran's cyber capabilities. Some of the CTAs work for the government and/or within IRGC directly. Others are part of affiliated groups, some of whom are ideologically aligned with the regime (such as the Iranian Cyber Army), and others who operate on a more contractual basis. Iran is well-known for using "proxies" in their offensive operations.

Two of Iran's more prominent APTs are APT 33 and APT 34. APT 33 (sometimes referred to as Refined Kitten or Elfin) tends to focus on the aviation, energy (targeting industrial control systems), and petrochemical industries and commonly uses both spear-phishing and more traditional malicious tactics like brute force attacks, password spraying, and file transfer protocol (FTP) exfiltration. They are widely believed to be responsible for the 2012 attack on Saudi Aramco that destroyed 35,000 computers. APT 34 (sometimes referred to as OilRig, Helix Kitten, or Cobalt Gypsy) is a cyber espionage group that has targeted multiple CI sectors and has shown a particular interest in the oil and gas industries. Bottom line, Iranian CTAs have already developed some collaborations with collectives in China and Russia (especially Russia currently), and as Tehran expands its political, military,[21] and economic cooperation with those countries, their cooperation in offensive cyber operations is also likely to accelerate.

State-sponsored

It is difficult to distinguish between nation-state and state-sponsored cyber threat actors because sometimes they are one-in-the-same. The aforementioned nation-states—China, Russia, North Korea, and Iran— are known for using "hackers for hire" and therefore these groups are state-sponsored groups. While it is difficult to definitively attribute any given cyber-attack to its source, in 2007, most experts believe Russia sponsored or employed hackers to mount a series of disruptive attacks—mainly distributed denial of service (DDoS), spamming, and website defacements—against Estonia after the country decided to move several WWII-era grave markers, including the Bronze Soldier of Tallinn. Then, a series of 2009 cyber-attacks against tech companies (known as Operation Aurora), including Google, are believed to have been executed by a Chinese state-sponsored collective of hackers.

Organized Crime

Cybercriminals continue to victimize Florida's citizens, businesses, and its critical infrastructure (CI) with ransomware, theft, and scams for financial gain. The overlay of organized cyber-crime potentiates the problem. In 2022, the FBI's Internet Crime Complaint Center (IC3) registered 800,944 complaints, with estimated losses exceeding $10B. Florida documented 42,792 victims with an accumulated loss of nearly $844.9M, placing the State in the #2 position nationally for the largest number of victims and dollars lost.[22] The most common reports were for phishing,

[21] Seligman, L. & Ward. A. (June 9, 2023). New U.S. intelligence shows Russia's deepening defense ties with Iran. Politico. Available at: https://www.politico.com/news/2023/06/09/united-states-security-council-russia-iran-weapons-00101191?cid=apn

[22] FBI's Internet Crime Complaint Center (2023). *Federal Bureau of Investigation Internet Crime Report: 2022*. Report: FBI Internet Crime Complaint Center.

personal data breach, and theft through non-payment/non-delivery, but investment fraud—with a large portion coming from cryptocurrency schemes—caused the highest losses—$3.3B. Organized criminals have expanded operations in the cyber domain, sometimes in collaborative transnational networks, deploying their tools within operational structures that are efficient, well-resourced—technically and financially—and have a global reach. Each of these advantages potentiates their tactical threat to U.S. CI.

CI's potential for high impact effects and high-yield financial gain makes them strategically attractive targets for organized cyber-crime. Ransomware is potentially the most problematic and costly tactic that cyber criminals use against CI given its ability to cause major disruption in sectors such as government and healthcare and in supply chains. Recent organized cyber-crime trends of particular concern include procurement attacks, supply chain attacks, multi-layered extortion methods, mobile malware, and a resurgence of distributed denial of service (DDoS) for ransom leveraging the reputation of well-known APTs to intimidate victims into compliance. Some criminal collectives have developed more sophisticated operational security measures. They continue to rely on grey infrastructure such as cryptocurrencies, virtual private networks (VPNs), and encryption services, and to use the Dark Web for communication, information sharing, and sales of stolen and illicit products and information. They have also increased their use of Wickr and Telegram, of anonymous cryptocurrencies, and of bartering/trading without any traceable financial exchange.[23]

Terrorists

The threat of cyber terrorism against critical infrastructure (CI) —especially by nation-states/proxies, non-state CTAs, and ideologically motivated lone actors—remains real. To date, the number and impact of such attacks against CI targets have been limited, however, most CI sectors have drawn the sustained attention of terrorist groups and lone actors. CI's potential for large-scale disruption and widespread public panic offers a strategic advantage to terrorist CTAs, especially within a framework of asymmetric conflict and competition. Cyber terrorist attacks are not hindered by geographical boundaries. They require fewer personnel and fewer resources than traditional human intelligence collection, terrorist attacks, or kinetic action and carry a lower risk of attribution or incidental harm to the actor's own assets.

Infrastructure systems can be disrupted or disabled by distributed denial of service (DDoS) attacks or even controlled with the introduction of malware. Ransomware can render systems and system-related information inaccessible to CI owners and operators. Maintenance access points often have limited security. Known vulnerabilities in standard IT components can be exploited. Because most infrastructure relies on the Internet and is highly networked and interconnected, it is possible for a single attack to generate extended ripple and cascading effects.[24] Cyber terrorism is an accessible and potentially effective instrument for extremist actors to gain informational advantage and advance their political or ideological objectives.

[23] Europol (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Report: Publications Office of the European Union, Luxembourg.

[24] Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. Article: *Cybersecurity*, *4*, 1-19.

Hacktivists

Hacktivism has been observed around the world and should be considered a potential threat to critical infrastructure (CI). Hacktivists are individuals or collectives who use their computing and hacking skills to protest perceived injustices or advance their political, social, or ideological objectives. They typically aim to disrupt rather than cause physical harm. Such disruption to CI systems, however, can lead to economic losses, loss of public trust, and have potential cascading effects on other sectors. For example, if a CTA believes that a CI entity or service provider is harming the environment, they can turn cyber resources against that entity and do immeasurable damage to their network/systems, adversely affecting their operations and reputation. Hacktivists typically target organizations or systems that symbolize or support causes they perceive as oppressive or corrupt. This often includes government agencies, corporations, and financial institutions. Common tactics and methods include distributed denial of service (DDoS) attacks, data breaches, information leaks/disclosures, and website defacements. The size, capabilities, and motivations of the individuals or groups determines the level of disruptive threat.

Insider

Insider threats continue to pose a persistent hazard to critical infrastructure (CI) in Florida and beyond.[25] An insider threat is generally regarded as "the threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States" [26] or "to do harm to the department's mission, resources, personnel, facilities, information, equipment, networks, or systems."[27] Insiders pose a unique cybersecurity challenge as CTAs because they have authorized access to systems (that they are using in unauthorized ways) and have detailed knowledge of those systems and their vulnerabilities. That access and knowledge can allow them to cause severe damage to critical systems, disrupt operations, steal sensitive information, or inflict physical destruction before being detected.

Insider threats can include intentional/malicious and unintentional actions. Malicious insider threats may arise from disgruntled employees or insiders recruited by external actors, often for financial gain. In fact, in a 2023 survey, more than a third (35%) of CI security leaders said they believe the global economic downturn is pushing more internal employees to turn to data theft

[25] The National Counterintelligence and Security Center (March, 2021). *Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective*. Report: The National Counterintelligence and Security Center. Available at: https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf; National Infrastructure Advisory Council (2020). *Insider Threat to Critical Infrastructures: Final Report and Recommendations*. Report: National Infrastructure Advisory Council. Available at: https://www.cisa.gov/resources-tools/resources/niac-insider-threat-critical-infrastructures-final-report-and
Hylender, C.C., Langlois, P., Pinto, A., & Windup, S. (2023). 2023 Data Breach Investigations Report (DBIR). Verizon Threat Research Advisory Center. Available at: https://www.verizon.com/business/resources/T4e5/reports/2023-data-breach-investigations-report-dbir.pdf

[26] See for example, CNSSI 4009-2015 from CNSSD No. 504 – Adapted, NIST SP 800-171 Rev. 2

[27] See for example, Cybersecurity Infrastructure Security Agency (n.d.) *Defining Insider Threats*. Website: Cybersecurity Infrastructure Security Agency. Available at https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

and sabotage.[28] In March 2021, for example, a Russian national was convicted of offering $1M to an employee of a U.S. electric car manufacturing company to inject malware into the company's network[29]. Unintentional insider threats typically stem from negligence, human error, or simply lack of awareness. Even if the system compromise is accidental, the losses and damage to the organization—or even to national security—can be substantial and persistent.

[28] Bridewell (2023). *Cyber Security in Critical National Infrastructure Organisations: 2023*. Research Report: Bridewell.

[29] The employee in this case did not accept payment or act against the company, but reported the encounter to security, ultimately leading to the perpetrator's arrest.

Cyber Threat Vectors

According to the 2022 *FBI Internet Crime Report*, out of the 479,181 victims of cyber-crime in the U.S. last year, 42,792 were Floridians, only second to California, resulting in $844.9M in statewide losses.[30] According to a Mandiant survey, "67% of respondents believe their senior leadership team underestimate the cyber threat to their organization."[31]

Phishing and Social Engineering

Phishing continues to be the number one vector utilized to deploy malware, ransomware, etc. According to the 2022 *FBI Internet Crime Report*, there were over 300K phishing attacks in 2022.[32] Phishing is primarily used by remote cyber threat actors (CTAs) and bots and has limited attribution. Phishing attacks can be targeted (spear-phishing or whaling) or non-targeted (random) attacks containing malware, such as ransomware. These attacks are conducted via emails, web-based "clickbait," and phone-voice calls, to name a few.[33] If "clicked," it can allow quick and significant access to digital systems with minimal effort from the attackers and is often the most lucrative method for financial gain. Phishing is the most common type of social engineering.

Social engineering is the use of deception to persuade a person to provide unauthorized access to a system or sensitive information that is useful to the CTA.[34] It can be accomplished physically (face-to-face) or over a medium, e.g., phone, email, etc. and is sometimes employed as a precursor to an offensive cyber-attack. Part of active system management for the people, processes, and procedures of an organization involves proactive management and visibility to deal with the complications these attacks present to an organization.

Cyber-Attacks/Probing

CTAs are constantly attacking and probing critical infrastructure (CI) networks for access points and vulnerabilities. A CTA's initial actions in planning a cyber-attack is called the reconnaissance phase. In this phase, the CTA starts looking at the system perimeter to find weaknesses/vulnerabilities to exploit for an attack.[35] This can be accomplished passively (collecting information without direct interaction) or actively (collecting information with direct

[30] FBI's Internet Crime Complaint Center (2023). *Federal Bureau of Investigation Internet Crime Report: 2022*. Report: FBI Internet Crime Complaint Center.

[31] Mandiant (2023). *Global Perspectives on Threat Intelligence*. Report. Mandiant.

[32] FBI's Internet Crime Complaint Center (2023). *Federal Bureau of Investigation Internet Crime Report: 2022*. Report: FBI Internet Crime Complaint Center.

[33] Fortinet (2023). *19 types of phishing attacks*. Website: Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

[34] Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, 102-113.

[35] Mazurczyk & Caviglione (2021). *Cyber reconnaissance techniques*. Article: ACM. Available at: https://cacm.acm.org/magazines/2021/3/250712-cyber-reconnaissance-techniques/fulltext

interaction) through physical (on-site) access, e.g., asking an employee what type of servers the company uses, or virtual (online) access, e.g., scouring external “Internet-facing” systems. Physical access may include looking at geospatial imagery, driving by, drone surveillance, or actions as simple as walking the site. Virtual access may include looking at perimeter firewalls, software applications, and other systems that can be used either to probe or breach the business systems. This is often accomplished anonymously with little potential for attribution. To identify reconnaissance activity, an organization can use cyber intelligence, cameras, active hunt methods, intrusion detection and prevention systems (IDS/IPS), blocked traffic logs, or other monitoring methods. The February 2023 cyber-attack on Tallahassee Memorial demonstrates that attacks against CI in Florida are not just speculative or hypothetical.[36]

Malware

Malware is “any software used to gain unauthorized access to IT systems in order to steal data, disrupt system services, or damage IT networks in any way.”[37] Malware is the primary vector that allows CTAs network access and phishing is the tactic used for deploying malware. More specifically, phishing campaigns enacted through large Spambots (computers designed to send mass emails) or targeted attacks against C-Suites, known as whaling, all have a common thread, which is the use of email to introduce malicious software that gives CTAs access to the network. This often happens very quickly without the user’s knowledge and is often detected only after it has been active within the network for some time. These attacks often have high success rates, providing the CTAs with substantial gain with minimal effort. [38]

The main types of malware are: Trojans (malicious code that imitates or is hidden within an apparently legitimate program); Rootkits (malware that allows CTAs to control a device remotely); Worms (malicious code that self-replicates as it spreads through the network); Adware (malware that delivers unwanted or malicious advertisements/SPAM); Denial of Service (DoS)/Distributed Denial of Service (DDoS) (malware designed to disrupt or disable a network server by overwhelming it with requests and traffic); Spyware (malware that intrusively collects user data); and Ransomware (malicious code that encrypts a victim’s/user’s data, denying access until a “ransom” payment is provided).

These programs all operate to collect data types, create remote connections, stage attacks, lock systems, and create access to meet the CTA’s objectives. This is a key reason networks need to be carefully monitored, architecturally resilient, and continuously improved to compete against these ever-evolving automated attack methods. CISA maintains a list of common malware

[36] Landi (2023). *Tallahassee hospital continues to operate offline, working with FBI to address 'IT security event'*. Article: Fierce Healthcare. Available at: https://www.fiercehealthcare.com/health-tech/tallahassee-hospital-takes-it-systems-offline-postpones-procedures-after-apparent-cyber

[37] CISA (2023). *Malware, phishing, and ransomware*. Website: CISA. Available at: https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[38] Amos (2022). *The evolution of malware*. Article: Cyber Talk. Available at: https://www.cybertalk.org/2022/03/15/the-evolution-of-malware/

strains, including their type, length of activity, method of delivery, resources, and mitigation strategies.[39]

Ransomware

Ransomware is a type of malware with a primary goal of financial gain. With ransomware, CTAs hold a user's data captive until a payment (ransom) is paid.[40] Because access to the blocked data is necessary for an organization to operate, CTAs have numerous types and levels of potential ransomware targets. There are countless variants of ransomware. According to the *2022 FBI Internet Crime Report*, LockBit, ALPHV/BlackCat, and Hive are the three top ransomware variants victimizing CI.[41] CI security leaders specifically report a significant increase in ransomware threats between 2022 and 2023.[42] Because ransomware is a form of malware, phishing is the number one method employed for deploying ransomware as well. The FBI's report lists Healthcare and Public Health, Critical Manufacturing, and Government Facilities as the top three CI sectors victimized by ransomware.[43]

Research & Development and Intellectual Property Theft

Florida is a prime target for research & development (R&D) and intellectual property (IP) theft because of the number of research universities and technology companies conducting R&D and relying heavily on IP. This creates an attractive opportunity for highly-sophisticated CTAs to target Florida. Florida is a national leader in R&D for space programs,[44] medical research,[45] and military research.[46] This makes protecting this research not only important for the state, but for the country and national security.[47] To remain competitive, Florida must look for new ways to protect their R&D-related digital information across all industry types. This will require new approaches to cyber defense and cyber intelligence to better understand the threats and protect

[39] CISA (2022). *Top 21 malware strains*. Website: CISA. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-216a

[40] CISA (2023). *Malware, phishing, and ransomware*. Website: CISA. Access at: https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[41] FBI's Internet Crime Complaint Center (2023). *Federal Bureau of Investigation Internet Crime Report: 2022*. Report: FBI Internet Crime Complaint Center.

[42] Bridewell (2023). Cyber Security in Critical National Infrastructure Organisations: 2023. Research Report: Bridewell.

[43] FBI's Internet Crime Complaint Center (2023). *Federal Bureau of Investigation Internet Crime Report: 2022*. Report: FBI Internet Crime Complaint Center.

[44] Space Florida (2023). *Florida is the unquestioned leader in the global aerospace industry*. Website: Space Florida. Available at: https://www.spaceflorida.gov/why-florida/

[45] Enterprise Florida (2023). Life Sciences. Website: Enterprise Florida. Available at: https://www.enterpriseflorida.com/industries/life-sciences/

[46] Enterprise Florida (2023). *Florida Defense Task Force*. Website: Enterprise Florida. Available at: https://www.enterpriseflorida.com/military-defense/florida-defense-support-task/

[47] NIST (2023). Cybersecurity for R&D. Website: NIST. Available at: https://www.nist.gov/cybersecurity/cybersecurity-rd

Florida's highly valuable R&D.[48] Again, phishing and social engineering are the primary tactics used to initiate R&D and IP theft.

Cyber Scams

According to the *FBI's Internet Crime Report* for 2022,[49] investment scams have taken the lead in cyber scams costing $3.31B, more than doubling the U.S. losses in 2021. Business email compromise (BEC) is the second most costly cyber scam at $2.7B. A BEC may look like this: a CTA pretends to be the CEO of a company and sends a carefully crafted email with a vendor's invoice containing incorrect routing and account numbers to the CFO for payment. Everything looks correct on the surface, so the CFO pays the vendor. This money never goes to the vendor but into the CTA's account. Tech support and call center scams have moved up to a distant third place at a cost of $800M. The FBI IC3 tracks 27 cyber-crime types, more than half of which are considered cyber scams. Persons over the age of 60 account for 69% of the victims for these scams,[50] and Florida has the highest proportion (just over one in five) of over-60 citizens of any state in the country. Again, phishing and social engineering are the primary methods employed to initiate cyber scams.

Artificial Intelligence and Quantum Computing

The rise of generative artificial intelligence (AI) has made AI the next major cyber threat to Florida and the nation, especially to CI operators and technology companies. As the CISA Director stated, if generative AI goes unchecked it has the potential of being an "extinction event" for humanity.[51]

AI in the modern world has taken on many different definitions. Historically, AI has referred to the imitation of all human behavior, not just spoken language, but vision, hearing, walking and other characteristics. In its modern context, however, the definitional rubric is less functional and more narrowly focused on machine learning algorithms. To date, no one has developed a sentient machine, which would be closer to the original context of what AI was defined to be.[52] Now that

[48] Select Committee on Artificial Intelligence (2023). *National artificial intelligence research and development strategic plan 2023 update*. Report: Select Committee on Artificial Intelligence. Available at: https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf

[49] FBI's Internet Crime Complaint Center (2023). *Federal Bureau of Investigation Internet Crime Report: 2022*. Report: FBI Internet Crime Complaint Center

[50] FBI's Internet Crime Complaint Center (2023). *Federal Bureau of Investigation Internet Crime Report: 2022*. Report: FBI Internet Crime Complaint Center.

[51] Graham (2023). Artificial intelligence's potential as an "extinction event" for humanity prompted CISA Director Jen Easterly to advise companies to "think about self-regulation" for product security and safety. Article: Nextgov. Available at: https://www.nextgov.com/emerging-tech/2023/05/ai-and-china-are-defining-challenges-our-time-cisa-director-says/386952/

[52] Marr (2018). *The key definitions of artificial intelligence (AI) that explain its importance*. Article: Forbes. Available at: https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/?sh=1c4125354f5d

we are redefining what AI is and is not, it is important to understand where we are and the future implications. This is why AI is one of the most widely discussed topics today around modern computing.

AI is transforming the nature of cybersecurity threats; there are already a number of concerning capabilities that exist and are being used today. For example, CTAs use generative AI to build more sophisticated and less vulnerable custom malware; to disrupt and compromise machine-learning-based threat detection software; to create audio and visual deep fakes that can amplify the effectiveness of social engineering attacks and malign influence operations; and to create highly realistic, personalized phishing and spear-phishing email messages that mimic a trusted source and are especially difficult for employees and authorized users to detect.[53]

Looking forward, the most significant AI developments will come from its integration with quantum computing capabilities. Current AI platforms are built on the traditional binary (1s and 0s) computing system. Quantum computing systems have an additional set of values between 1s and 0s that exponentially increase their computational power. For the purpose of comprehending potential AI cybersecurity threats, it is not necessary to understand the details and complexities of quantum computing. The fundamental implication is that quantum dramatically expands AI capabilities with speeds that far exceed those produced by binary computing.[54]

Quantum computing is capable of breaking all binary cryptography as we currently know it. This means, should a quantum capable system target cryptographic security, no encryption currently used in industry is secure.[55] The combined impact of quantum computing and machine learning/AI will change the modern cyber threat landscape much more quickly than evolving changes in binary computing systems. Technological developments are already outpacing government and industry abilities to develop effective policies or to think through the ethical, operational, and societal implications of those changes. Tech companies and researchers are using "open-source" interactions with ChatGPT (OpenAI), Bard, Jasper, Bing, ChatSonic, etc.to leverage large segments of the population to make their AI become more human-like more quickly.

[53] Renaud, K., Warkentin, M., & Westerman, G. (2023). From ChatGPT to HackGPT: Meeting the Cybersecurity Threat of Generative AI. MIT Sloan Management Review, 64(3), 1-4.

[54] IBM (2023). *What is quantum computing?* Website: IBM. Available at: https://www.ibm.com/topics/quantum-computing

[55] DHS (2021). DHS releases guidance to mitigate security risks with the advancement of quantum computing. Article: DHS. Access to: https://www.dhs.gov/news/2021/10/04/dhs-releases-guidance-mitigate-security-risks-advancement-quantum-computing

Best Practices for Protecting Critical Infrastructure

Below is a list of tips (Best Practices) that may improve cyber defense for Florida's critical infrastructure (CI):

Prioritize Cyber Intelligence

Cyber intelligence should serve as the first line of prevention and mitigation against cyber threats. Cyber intelligence provides the who, what, when, where, why, how, so what, and possible solutions to cyber events. Cyber intelligence can potentially anticipate cyber events, and therefore assist in preventing them, and help mitigate incidents that do occur.[56]

Conduct Risk/Vulnerability Assessments and Cybersecurity Planning

Risk is a function of threats and vulnerabilities. Comprehensive and continuous assessments are essential to identify threats (hazards) and vulnerabilities (weaknesses) in a dynamic environment and to anticipate potential consequences. Those assessments will reveal the organization's level of cyber defense maturity, which the organization can use to inform its cybersecurity planning and investments.[57] A common vulnerability in CI systems is over-reliance on legacy technology. Older systems often cannot support newer updates and patching, so it is important that device upgrades are considered in cybersecurity investment plans. With a more secure foundation, the organization will be better positioned to incorporate routine vulnerability assessments and patch management plans.[58] The ability to understand the organization's cybersecurity posture is paramount to planning ways to improve its ability to deal with cyber threats. Conversely, effective planning will shape the organization's cybersecurity posture as well. Cybersecurity planning should include a full range cyber defense activity from prevention to incident response to continuity and recovery efforts, all designed specifically to meet the organization's requirements. [59]

[56] Borum, R., Felker, J., Kern, S., Dennesen, K. & Feyes, T. (2015). Strategic Cyber Intelligence. Article: *Information Management and Computer Security*, 23 (3), 317 – 332. DOI 10.1108/ICS-09-2014-0064
Gentry, J. A. (2022). Cyber Intelligence: Strategic Warning Is Possible. Article: *International Journal of Intelligence and CounterIntelligence,36*(3), 729-754.
Kure, H., & Islam, S. (2019). Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. Article: Journal of Universal Computer Science, 25(11), 1478-1502.

[57] SAFECOM (2023). Guide to getting started with a cybersecurity risk assessment. Report: SAFECOM. Access at: https://www.cisa.gov/sites/default/files/video/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508-r1.pdf

[58] Global Cybersecurity Alliance (2021). The top 7 operational technology patch management best practices. Website: Global Cybersecurity Alliance. Available at: https://gca.isa.org/blog/the-top-7-operational-technology-patch-management-best-practices

[59] Cohen (2023). *Throwback attack: Iranian-backed OilRig targets critical infrastructure in the middle east.* Article: Industrial Cybersecurity Pulse. Access at: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-iranian-backed-oilrig-targets-critical-infrastructure-in-the-middle-east/

Inventory and Prioritize Assets

If an organization does not know what it has, it is impossible to secure. An accurate asset inventory is both an operational and a cybersecurity requirement. Understanding all devices and software on the network will allow issues to be quickly identified and efficiently corrected. It will also allow an organization to align the allocation of security resources with the value/criticality of any given asset. While an organization can strive to defend and protect everything, not everything–if done effectively–will be protected equally well. By aligning defense and asset priorities, the organization will reduce costs and better protect its most valuable or sensitive data. Inventory activity should include a review of process control system (PCS) components and should be expanded to include any computer systems and network devices on the operational technology (OT) and business networks that could interact with supervisory control and data acquisition (SCADA) systems including the data flow system (DFS). Storing the inventory in a database is the recommended approach and there is software available (both commercial and open source) for this purpose. For example, Rockwell FactoryTalk AssetCentre might be used to manage the program logic controller (PLC) inventory, provide a central repository for programs, and add additional security features. At a minimum, an asset inventory should include device type (e.g., PLCs, remote terminal units (RTUs), switches, servers, radios, and firewalls) software version; location; serial number; MAC addresses, IP addresses and host names; device function; and whether the device is upgradable or updatable.

Create a Cybersecurity Culture - People, Process, Procedure

Maintaining a secure posture is one of the most overlooked aspects of cybersecurity. Cybersecurity must be built into the CI culture in the same way that safety has been embedded to the CI industry: by ensuring all personnel are trained, aware, and actively participating with cybersecurity in mind; processes are continuously improving and maintained; and procedures are in place for successful cybersecurity prevention and incident response programs.[60]

CI organizations are encouraged to develop an "all hands" approach to cybersecurity, which includes cybersecurity awareness training with realistic, scenario-based, simulation exercises.[61] Social engineering and phishing, technically a type of social engineering, are too often effective.[62] A "Do not click the link!" rule can be helpful but will not be sufficient. Users must be inoculated against common deceptive tactics. A strong cybersecurity posture requires more than a "one and done" training program. Threat awareness and management programs must adapt to an ever-changing threat environment and build in accountability processes to ensure that

[60] Carpenter (2023). Why security culture is key to cybersecurity resilience. Article: Forbes. Available at: https://www.forbes.com/sites/forbesbusinesscouncil/2023/02/21/why-security-culture-is-key-to-cybersecurity-resilience/?sh=4db271717f8f

[61] Chowdury, N., & Gkioulos, V. (2021). Cybersecurity training for critical infrastructure protection: A literature review. Article: Computer Science Review, 40, 100361.

[62] Back, S., & LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. Article: *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 1-4.

the trained principles are put into practice. Cybersecurity awareness is so important that it has a month (October) dedicated to its promotion.[63]

Enforce Strong Access Controls

Access controls, such as requiring strong passwords and multifactor authentication (MFA), contribute to a good defensive foundation. But those polices are only useful to the extent that they are enforced and regularly reviewed and updated.[64] Following the Principle of Least Privilege (giving to each user the lowest level of access and fewest privileges needed to perform their assigned functions) and conducting regular access reviews will further strengthen the ability of access controls to mitigate the level of intrusion and possible damage if an account is compromised. The "Least Privilege" approach also harmonizes with and supports the movement in CI sectors toward a Zero Trust model.[65] This ensures that system access is compartmentalized in a way that prioritizes the security of the most critical system assets.

Apply a Zero Trust Framework

The Zero Trust Maturity Model[66] is becoming a standard of practice for critical systems architecture. Industrial Control Systems (ICS) architectures adapt well to this model because of the often-static IP and known communication requirements within these systems. The Zero Trust Model forces organizations to actively manage their operational technology (OT) environments, by knowing what is on their networks, how it is communicating, where it is communicating, and where it should not be communicating.[67] "Zero Trust" only allows known communications on the networks, which enhances security. A positive side-effect of zero trust implementation is that it helps significantly in operational troubleshooting and reduces the communications around multi-cast traffic that plague these networks. Overall, CI networks are ideally situated to support a Zero Trust Model and implementing it often increases organizational efficiency.

Patch All Systems

CI organizations should prioritize patching based on known exploited vulnerabilities. When vulnerabilities are identified and "patches" to mitigate them are disseminated, it is essential that

[63] CISA (2023). *Cybersecurity awareness month*. Website: CISA. Available at: https://www.cisa.gov/cybersecurity-awareness-month

[64] Cohen (2023). *Throwback attack: Iranian-backed OilRig targets critical infrastructure in the middle east*. Article: Industrial Cybersecurity Pulse. Available at: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-iranian-backed-oilrig-targets-critical-infrastructure-in-the-middle-east/

[65] Palo Alto Networks (2023). What is the principle of least privilege? Article: Palo Alto Networks. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege

[66] CISA (2023). *Zero Trust Maturity Model: Version 2.0.* Report: CISA. Available at: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[67] Boumhauout (2020). *Towards Zero Trust For Critical Infrastructure: Rethinking The Industrial Demilitarized Zone.* Paper: Massachusetts Institute of Technology.

all systems, including operating systems, software, firmware, and applications, be updated as soon as possible. When feasible, automatic patching is the best approach to ensure uniform coverage and compliance. For others, a patch management process and/or policy should be in place to identify available patches as they emerge, convey the patch requirements to pertinent users, and follow-up and enforce the update.[68] System patching is important to ensure that both operational and cybersecurity weaknesses are being addressed quickly and safely. The goal of patching is not only to support cybersecurity (though it has a large role in this regard), but also to ensure that operations continue to function efficiently to reduce waste (either time or efforts) for the organization.[69]

Secure and Monitor Remote Access

All information technology (IT) and operational technology (OT) networks that support remote desktop protocols (RDP), virtual network computing (VNC) and other remote access protocols are potentially exploitable by CTAs across the attack lifecycle and should be secured.[70] When possible, remote access protocols should not be utilized and should be blocked from usage. If remote access is an operational requirement, ensure only those with authorized credentials use it and monitor their usage.

Implement Architectural Resiliency and Network Segmentation

Critical system architectures in the state of Florida and beyond are often outdated (from the 1990s and early 2000s) and sometimes lack consistency. CI owners and operators should build resiliency into networks to counter those vulnerabilities.[71] A single firewall, especially one that is improperly configured, within an integrated architecture offers insufficient protection. Increased use of Linux-based servers and commercial software in Industrial Control Systems (ICSs), cloud computing, remote access requirements, and the increase in multi-frequency remote communication have created new vulnerabilities for attackers to gain persistent network access.[72] Segmenting the network to isolate critical systems, will mitigate the depth and scope of potential breaches and restrict attackers' lateral movement within the system.

[68] Cohen (2023). *Throwback attack: Iranian-backed OilRig targets critical infrastructure in the middle east*. Article: Industrial Cybersecurity Pulse. Available at: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-iranian-backed-oilrig-targets-critical-infrastructure-in-the-middle-east/

[69] Intel (2023). What is patch management? Website: Intel. Available at: https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/patch-management.html

[70] Lockheed Martin (2015). *The Lockheed Martin Cyber Kill Chain*. Report: Lockheed Martin. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[71] CISA (2019). *A guide to critical infrastructure security and resilience*. Report: Cybersecurity and Infrastructure Protection Agency. Available at: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf
Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Article: *Information & Computer Security, 30*(2), 255-279.

[72] Cyberark (2022). Strengthening critical infrastructure security mitigate risk with privileged available management. Book: Cyberark Software. Available at: https://www.cyberark.com/resources/ebooks/strengthening-critical-infrastructure-security

Create Secure Backups and Plan for Continuity and Recovery

CI security professionals should ensure that critical data and systems are backed up regularly, tested for reliability, and securely stored. They should create and test a detailed plan for continuity of operations, disaster recovery, and recovery/restoration of critical support systems in the event a serious attack or breach occurs. Because onsite backup recovery after ransomware attacks is sometimes known to fail, it is useful to consider tested off-site backups.[73]

Continuously Monitor the Network

CI security professionals should continuously monitor network and system activity for signs of compromise or anomalies using security monitoring tools and technologies, including security information and event management (SIEM) solutions.[74] Security monitoring has grown significantly in recent years with the development of next generation, "full stack" systems that monitor from the Internet perimeter to the end-point computer system. These robust systems are redefining the ability to monitor all the devices on the network in sophisticated ways. They are quickly moving beyond the capabilities of older SIEM systems to a full network approach. This transition is allowing teams to deploy single vendor products that secure, patch, monitor, identify, detect, respond, and notify digital threats all within a single solution.[75]

Establish Cybersecurity Governance

CI organizations should develop a comprehensive cybersecurity governance strategy that integrates with, and defines risks to, the organization's operations. These strategies should establish clear procedures for threat prevention and mitigation; designate which personnel should be making which decisions and performing which functions (and when); and outline operational frameworks for accountability and oversight.[76] The lack of adequate governance programs is one of the most common causes of compliance failure in the critical system industry. Without a

[73] Palo Alto Networks (2023). 2023 Unit 42 ransomware report. Report: Palo Alto Networks. Available at: https://start.paloaltonetworks.com/2023-unit42-ransomware-extortion-report

[74] Cohen (2023). *Throwback attack: Iranian-backed OilRig targets critical infrastructure in the middle east*. Article: Industrial Cybersecurity Pulse. Available at: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-iranian-backed-oilrig-targets-critical-infrastructure-in-the-middle-east/

[75] Palo Alto Networks (2017). Next-generation security platform. Flyer: Palo Alto Networks. Available at: https://betta-security.com.ua/downloads/paloalto/Palo%20Alto%20NGFW_Betta%20Security.pdf

[76] CISA (2023). *Cybersecurity Governance*. Website: CISA. Available at: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance; Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. *EDPACS: The EDP Audit, Control, and Security Newsletter*, *63*(6), 1-22. Article: Research Gate. Available at: https://www.researchgate.net/profile/Maleh-Yassine/publication/343837946_A_Maturity_Framework_for_Cybersecurity_Governance_in_Organizations/links/611d4268169a1a01030ee5e3/A-Maturity-Framework-for-Cybersecurity-Governance-in-Organizations.pdf; Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research*, *16*(4), 490-513.

roadmap for organizational accountability, it is hard to achieve a successful cybersecurity program. Clear procedures and careful oversight are necessary for long-term success.[77]

Establish Incident Detection and Response

Timely incident detection and response is key to an organization's cybersecurity success. Using tools such as intrusion detection and prevention systems (IDS/IPS) can provide an initial line of defense. Incident response procedures should include mitigation tactics that are immediately employed in the event of an intrusion and guidance on how and to whom any incident-related information should be provided.

Hunt the Network

Beyond using automated tools for monitoring the network, security analysts should regularly hunt (search through the network to find malware, spyware, ransomware, etc.) through the systems and logs to ensure CTAs are not already in the network. Active threat hunting is done by the most mature organizations. Identifying security risks requires visibility into and knowledge of the networks.[78] A good starting point for threat hunting is examining packet captures from key boundary switches via span-ports or a tap device. Once the packet data are captured, analysts can conduct a nodal analysis (using tools such as NSA's "Grassmarlin," available free on GitHub[79]) to see how the traffic transits the network and if it is making any unexpected system connections, especially to potential command and control networks. Thorough threat hunting will help to identify any current malware or threats on the network to ensure there is a clean foundation on which to build active monitoring threat programs. It also provides a baseline of network activity, which can serve as a reference point for identifying future anomalous signals of malicious activity before an attack occurs.

Establish Partnerships and Share Information

CI owners and operators are encouraged to engage with government agencies (such as participating in in CISA's *Shields Up*;[80] the Department of Energy's Cybersecurity Risk Information Sharing Program or CRISP;[81] and the Department of Transportations' ITS

[77] CISA (2023). *Cybersecurity governance*. Website: CISA. Available at: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance

[78] IBM (2023). *What is threat hunting?* Website: IBM. Available at: https://www.ibm.com/topics/threat-hunting

[79] NSA (2017). GRASSMARLIN. NSA Tool: GitHub. Available at: https://github.com/nsacyber/GRASSMARLIN

[80] CISA (2023). *Shields Up!* Website: CISA. Available at: https://www.cisa.gov/shields-up

[81] U.S. Department of Energy (2023). *Cybersecurity Risk Information Sharing Program (CRISP) Fact Sheet*. Report: U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. Available at https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet_508.pdf

Cybersecurity Research Program[82]), cybersecurity research centers, CI sector peers (particularly sector-specific information sharing and analysis centers or ISACs[83]), and industry and private sector threat intelligence/information sharing platforms, all of which can increase situational awareness of emerging threats and enhance their ability to prevent and anticipate potential security incidents.

Do Not Pay the Ransom

Florida law prohibits state agencies from paying CTAs cyber ransoms.[84] The FBI discourages paying ransom to CTAs but suggests reporting any ransomware attacks to the FBI's Internet Crime Complaint Center (IC3) and the Cybersecurity & Infrastructure Security Agency (CISA).[85]
IC3: https://www.ic3.gov
CISA: https://www.cisa.gov/stopransomware

Conclusion

We assess the current, overall cyber threat risk to Florida's CI as MODERATE (*on a scale of low, moderate, and high[86]). Florida's critical infrastructure is not immune to cyber threats from a

[82] U.S. Department of Transportation (2023). ITS Cybersecurity Research Program. Website: U.S. Department of Transportation, Intelligence Transportation Systems Joint Program Office. Available at: https://www.its.dot.gov/research_areas/cybersecurity/

[83] National Council of ISACs (2023). Website: National Council of ISACs. Available at: https://www.nationalisacs.org/

[84] Elam, E. & Wanger, B.(2022). Florida prohibits state agencies from paying cyber ransoms. Florida Bar News. The Florida Bar. Available at: https://www.floridabar.org/the-florida-bar-news/florida-prohibits-state-agencies-from-paying-cyber-ransoms/

[85] FBI's Internet Crime Complaint Center (2023). *Federal Bureau of Investigation Internet Crime Report: 2022*. Report: FBI Internet Crime Complaint Center.

[86] **Low Risk**: Minimal or low probability of a serious adverse cyber event occurring. The potential exists for malicious activity, but typically no such (or only insignificant) unusual activity has been identified that targets the CI sector or the likely consequences of suspected activity are not severe, easily manageable, and would be expected to have limited adverse effects on CI operations, assets, and individuals (NIST Low Impact).
Routine preventive measures and monitoring are typically sufficient.
Moderate Risk: Moderate probability of a serious adverse cyber event occurring. Some malicious activity and/or exploits that target the CI sector have been identified, and risks to the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect (moderate levels of damage or disruption) on CI operations, assets, and individuals, but not involving loss of life or serious life-threatening injuries (NIST Moderate Impact).
Enhanced monitoring, defensive measures, and situational awareness may be required.
High Risk: High probability of a serious adverse cyber event occurring. Significant malicious activity and/or exploits that target the CI sector have been identified, and risks to the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effects (widespread level of damage or disruption) on CI operations, assets, and individuals, including loss of life or serious life-threatening injuries.
Immediate and comprehensive measures, including intensive monitoring, defensive measures (possibly isolating critical systems/networks), mitigation strategies, and situational awareness, are necessary.

range of actors (CTAs) pursuing cyber-attacks, probing systems, deploying ransomware, stealing R&D and IP, and conducting cyber scams, but they can take precautions to reduce their risk. Using effective cyber intelligence to better understand the threats to one's sector and an organization's own threat/attack surface, enhances the security of Florida's critical infrastructure. Employing intelligence-driven cyber threat prevention and mitigation techniques such as cybersecurity awareness training, multi-factor authentication, patching, and architectural resilience can greatly reduce the likelihood of a successful cyber-attack and mitigate the damage from any breaches that do occur.

Longer Term Recommendations

1. Create a state **cyber intelligence center**, Florida Cyber Intelligence Center (FCIC), to share cyber threat intelligence and information with public (e.g., government) and private (e.g., critical infrastructure) entities across the state. (see FCIC Pitch Paper)

2. Create a state **critical infrastructure cybersecurity lab and training facility**. An accessible, state-of-the-art training environment is needed to equip personnel to be able to build and maintain secure CI architecture and protect CI networks throughout the State.

3. Create a statewide critical infrastructure "**cyber threat warning system**" dashboard (can be a mission for the FCIC) using a stoplight scheme (red, yellow, green: red = imminent threat, yellow = potential threat, green = no known significant threat) or some other intuitive method for communicating risk and warnings. All appropriate entities could access and monitor the dashboard.

Example:

🔴

Healthcare and Public Health Sector
Supporting evidence: Tallahassee Memorial incident

🟡

Financial Services Sector
Supporting evidence: Continued probing across financial industry

🟢

Water and Wastewater Systems
Supporting evidence: N/A

4. Produce a periodic (e.g., daily, weekly, monthly, quarterly, and/or annual) **cyber intelligence report** for the State (can be a mission of the FCIC).

Sources for the cyber intelligence report could include:

- CISA Alerts & Advisories
- Information Sharing and Analysis Centers (ISACs) information
- Cyber Threat Intelligence (CTI)
- Reports and feeds from cyber intelligence companies, e.g., CrowdStrike, Mandiant, RecordedFuture, Tripwire
- Open-source news reporting and event aggregation/curation
- Tools, e.g., MITRE ATT&CK Framework, STIX, TAXII

Headings for the cyber intelligence report could include:

- Executive Summary
- Current Cyber Threats and Actors

- Indicators of Compromise (IOCs)
- Common Vulnerabilities and Exposures (CVEs)
- Cyber Threat Trends
- Recommended Prevention/Mitigation Techniques

Sun Tzu's adage from 2,500 years ago is just as relevant today and reflects the strategy underpinning an intelligence-driven approach to cyber defense: *"Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy, but know yourself, your chances of winning and losing are equal. If ignorant both of the enemy and of yourself, you are certain in every battle to be in peril."* [87]

[87] Tzu, S. (1971). *The art of war*. Book: Oxford University Press. p. 84.