BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 22-100 **November 2022, Issue #89**

BusinesSafe Sector Highlight - Critical Manufacturing

The critical manufacturing sector encompasses manufacturing that is vital to the longevity and prosperity of the U.S. economy. The manufacturers in this sector are responsible for processing the raw materials and producing materials and electrical components for a variety of equipment including trucks, commercial ships, aircraft, rail cars, and their supporting components. Florida is home to many aerospace, fabricated metal, electronics, industrial machinery, and equipment manufacturing companies. A disruption to these manufacturers may cause significant issues with many other sectors which rely heavily on the products produced by critical manufacturing entities.

Criminal Activity

- **Intellectual Property theft**
  Intellectual property theft is when a person or company acquires, through illegal means, legally protected ideas, creative expression or inventions from another individual or company. The majority of intellectual property theft is done to gain a competitive advantage in a field. Some criminals may use company employees or contractors to knowingly or unknowingly steal information. Criminals may also use cyberattacks such as phishing, ransomware, network intrusion, and others to exfiltrate proprietary information to hold or sell for profit.
  One in Five Manufacturing Firms Targeted by Cyberattacks
  Former U.S. Military Pilot Admits Acting as Paid Agent of China and Lying on National Security Background Forms

- **Foreign State Cyberattacks**
  Many of the processes used in the critical manufacturing sector are operated using interconnected information technology (IT) and operational technology (OT) networks. Foreign state actors acting at the direction of a foreign government may use cyberattacks on U.S. manufacturing companies in an effort to disrupt operations or carry out cyber espionage to help a foreign government gain industry advantage. Geopolitical tensions and conflicts may increase the risk of possible cyberattacks in the manufacturing sector. Tactics used in the past by foreign state actors include phishing, malware, distributed denial of service, compromising remote desktop protocol, and others.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8563 Approval: FL8651, HSEC:1, 2, 7, FSIN:1.2, 1.3, 3.1, FFC:1, 2, 6.1, 6.9

Russia Is Suspect In Cyberattack That Will Force Toyota To Shut Down Plants In Japan
Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Other Threats and Hazards

- **Natural disasters**
  Florida faces yearly threats of major hurricanes that have the potential to inflict serious damage on these vital manufacturers. While many critical manufacturing companies have built their facilities to withstand the high winds and flooding of the storms, they remain particularly vulnerable to power outages and worker shortages.
  Rebuilding Florida after Ian may be slowed by labor shortage
  Floridians could face weeks without power if Ian leaves grid 'beyond repair'

Mitigation Strategies

- To defend against cyberattacks companies can implement strategies like multi-factor authentication, segregate networks, update and upgrade software continuously, and actively manage systems and configurations.
- It's unrealistic to monitor every employee but behavior analytics solutions can monitor typical employee actions, such as odd work hours or irregular data spikes, as well as limiting access to only required systems and files.
- Companies should implement a plan of action for resuming operations following a natural hazard.

Resources:

- The Cybersecurity and Infrastructure Security Agency offers information on the Critical Manufacturing Sector as well as other resources to help employees identify and report suspicious activity and behaviors.
- The National Security Agency offers a list of the Top 10 ways to mitigate cyberattacks.
- If your organization experiences a data breach, network intrusion or ransomware attack, contact your local police department, the Florida Department of Law Enforcement, or the nearest Federal Bureau of Investigation (FBI) field office.
- For information and resources related to cybersecurity mitigation and reporting users can visit Shields Up and StopRansomware.gov
- "**If You See Something, Say Something®**" – Report suspicious activity to your local law enforcement agency, on the Florida Department of Law Enforcement website using Florida's See Something, Say Something Tool Kit, via the Florida See Say app, or by calling 855-FLA-Safe. In an emergency, call 911.
- The Intellectual Property Rights Center, a division of the Department of Homeland Security, provides an online form to report intellectual property theft.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8563 Approval: FL8651, HSEC:1, 2, 7, FSIN:1.2, 1.3, 3.1, FFC:1, 2, 6.1, 6.9