BUSINESSAFE

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 21-118 **October 2021, Issue #61**

BusinesSafe Highlight: Communications Sector

The communications sector is integral to business operations, public safety, and the U.S. government. It provides individuals and businesses with reliable interconnected systems for information exchange. Protecting the physical and data security of this sector is integral due to its interconnectedness with other critical infrastructure sectors, which rely on it to provide essential services used for daily business operations and emergency response.

Criminal Activity

Criminal actors may target the communications sector either to commit theft or disrupt operations. Operation disruptions can happen when criminal actors attack assets and equipment, steal necessary operating components, or commit cyberattacks. Cyber criminals may also use multiple types of cyberattacks to try to obtain proprietary information.

1. **Cyberattacks -** The communications sector's reliance on technology makes it a target for cyber criminals. Ransomware, distributed denial-of-service (DDoS), phishing, and malware are just a few types of attack types used by cyber criminals to disrupt operations or steal sensitive information. Foreign states may also target the communications sector to carryout cyber espionage on other governments and their critical infrastructure assets. Many companies work with the U.S. Government to ensure cyber security protocols are up to date and to create plans to help mitigate cyberattacks.
   Russian internet firm Yandex hit by major cyber attack
   Hackers Target Telecom Companies to Steal 5G Secrets

2. **Targeted attacks** - Criminal actors may use physical attacks to harm communications sector assets and businesses. Physical attacks can include the use of improvised explosive devices (IEDs) and arson. These types of attacks can cause prolonged service outages, disrupt business operations harm employees, and impact other sector operations.
   Northern Michigan Man Arrested in Connection with Pipe Bombs Left at Cell Phone Stores
   77 cell phone towers have been set on fire so far due to a weird coronavirus 5G conspiracy theory

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us

Author: FL8642, Approval: FL8600, HSEC: 1, FSIN: 1.1.1, 1.1.2, 1.2.1, 2.6.1, 2.14.3, 3.7.3 FFC: 1.2, 1.3, 1.4, 1.8, 6.3, 7.3

3. **Theft –** Communication assets and businesses are often targeted by criminals intending to steal critical operating components. Communication assets such as cell towers are scattered across the U.S., and often placed near public areas which make them an attractive target for criminals. Theft of components from these assets can lead to operation delays, shut downs, and costly repairs. Many businesses implement multiple security measures to assist with deterring theft.
   AT&T reports $32,000 in property stolen at cell tower site
   T-Mobile customers may lose service after $10,000 in copper wiring, cables stolen from Wake Forest cell tower

Resources

The Cybersecurity and Infrastructure Security Agency (CISA) provides information and links to resources on the Communications Sector.

The Federal Communications Commission offers information, events, and resources on the communication sector and provides resources for individuals and businesses to file complaints on their website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC: 1, FSIN: 1.1.1, 1.1.2, 1.2.1, 2.6.1, 2.14.3, 3.7.3 FFC: 1.2, 1.3, 1.4, 1.8, 6.3, 7.3