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 21-113 **September 2021, Issue #60**

BusinesSafe National Insider Threat Awareness Month

September is National Insider Threat Awareness Month. Insiders, such as current or former employees, consultants or contractors, often have authorized access to a company or organization's intellectual property, operating procedures, and facilities. Insiders can become a threat when an individual with authorized access uses their knowledge of an organization, or their access to proprietary information or secure areas to do harm to the security of that organization either willingly or unwillingly. Insider threat incidents can cost organizations time, money, resources, customers, and disrupt operations or cause harm. Organizations can take steps to mitigate the potential for insider threat incidents including implementation of security measures, looking out for behavioral indicators, and ongoing training.

Intellectual Property Theft – Insiders often have access to proprietary intellectual property such as inventions, ideas, trade secrets, and other information or property owned or created by an organization. Some bad actors may steal intellectual property for financial gain or a competitive edge, which can cause long term harm. Although many organizations take steps toward safeguarding their information and property, there is the potential for individuals with authorized access to circumvent these safeguards.
Chemist Convicted Of Stealing BPA-Free Can Liner Trade Secrets For A Chinese Firm
Former CEO And COO Of JHL Biotech Convicted Of Conspiracy To Steal Trade Secrets And Commit Wire Fraud Exceeding $101 Million

Sabotage - Insiders with access to computer networks and systems may use this access to disrupt company operations, which can cost the company time and money to recover. Sabotage can range from physical harm or disruptions to theft of an organization's information intended to cause harm Insiders can also use this access to attempt to harm customers and other employees by manipulating operating systems connected to the organization's network. Many organizations protect against this threat by implementing strong cyber security policies and awareness training and putting in place processes to promptly remove access granted to former employees or contractors.
San Jose Man Sentenced to Two Years Imprisonment for Damaging Cisco's Network
Sacked Employee Deletes 21GB of Credit Union Files

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC: 1, 4, 7, FSIN: 1.1, 1.10, 1.14, FFC: 1.1, 3.8.5, 3.9, 4.6, 6.1

Unintentional – An insider threat incident is not always done intentionally or maliciously. A criminal actor may exploit or trick a trusted insider into sharing sensitive information or providing access to secure areas or networks. This can happen through cyberattacks, including phishing incidents where the insider clicks on a malicious link, theft or other scams and fraud. Additionally, sensitive information can be released to unauthorized users through negligence, a breach in security protocols or inadvertent disclosures. Many organizations use continued employee education and IT security to help mitigate unintentional insider threat incidents.
3 Charged in Massive Twitter Hack, Bitcoin Scam
The Private Data Of 24 NHS Employees Have Been Caught Up In A Data Breach, Reports Reveal.

Resources

The National Counterintelligence and Security Center (NCSC) offers information and training resources to assist organizations in understanding and mitigating insider threats on their National Insider Threat Awareness Month website. NCSC also offers specific guidelines for Insider Threat Mitigation for U.S. Critical Infrastructure Entities.

The Cybersecurity and Infrastructure Security Agency (CISA) offers insider threat mitigation tools and resources to assist organizations with understanding and creating policies to protect their organizations.

The FBI gives a guide for organizations to assist with Identifying, Assessing, and Managing the Threat of Targeted Attacks.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC: 1, 4, 7, FSIN: 1.1, 1.10, 1.14, FFC: 1.1, 3.8.5, 3.9, 4.6, 6.1