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 23-061 **May 2023, Issue #103**

BusinesSafe Highlight – Insider Threat

An insider threat is an individual, usually an employee, who may use his or her authorized access, wittingly or unwittingly, to do harm to the security of an agency or department. Insiders may be current or former employees, partners, consultants, or contractors. Insiders may have access to important organizational information and may have more opportunities to exploit this information than external actors. Insider threat incidents like data or trade secret theft, destruction of computer systems, or network sabotage, can result in billions of dollars in damages each year. Threats to domestic security evolve over time but insider threat remains a concern for all organizations. Without proper security measures and training, those with access to important information or equipment may knowingly or unknowingly expose their organizations to potentially dangerous situations.

Types of Insider Threats

There are three major types of insider threats. These include unintentional threats, intentional threats, and "other" threats:

Unintentional threat:

- An insider can expose an organization to a threat due to negligence or carelessness. These insiders are typically familiar with security and/or IT policies but ignore them for various reasons, albeit unintentional. This creates risks for the organization.
- An insider can cause unintended risk to an organization by mistyping an email address and accidentally sending sensitive information to the incorrect party, unknowingly clicking on a malicious hyperlink, falling victim to a phishing email, or improperly disposing of sensitive documents.

Intentional threat:

- An insider could have malicious intent to harm an organization. This could be for personal benefit or to act on a grievance. Actions can include leaking sensitive information, harassing associates and colleagues, sabotaging equipment/technology, perpetrating physical violence, or stealing intellectual property.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8888, Approval: FL8900 , HSEC: 1, 4 FSIN: 1, 2.14, 3 FFC: 1, 4.1, 4.4, 6

"Other" threat:

- A malicious insider could collude with a malicious external threat actor to compromise an organization. Many of these incidents involve cybercriminals recruiting an insider to enable fraud, intellectual property theft, and/or espionage.
- Third-party threats can consist of contractors or vendors who are not formal employees of an organization, but have been granted some level of access to an organization's facilities or systems.

How to Mitigate Insider Threats

1. Identify and focus on critical assets, data, and services that the organization deems as valuable.
2. Monitor behavior of employees, contractors, and vendors to detect and identify trusted insiders who breach the organization's trust.
3. Assess threats to determine the level of risk of identified persons of concern.
4. Manage the entire range of insider threats. This includes implementing strategies focused on parts of the organization vulnerable to an insider threat.
5. Engage individual insiders who are potentially on the path to harming the organization, if it be intentionally or unintentionally.

Resources

- Cybersecurity & Infrastructure Security Agency (CISA) provides an excellent guide for mitigating insider threats.
- CISA also gives an overview of insider threats, including definition, detecting and identifying, assessing, and managing.
- The Interagency Security Committee (ISC) provides guidance on how agencies/organizations can develop a workplace violence plan.
- The Carnegie Mellon Software Engineering Institute provides a study on insider threats to computer systems in critical infrastructure sectors.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8888, Approval: FL8900 , HSEC: 1, 4 FSIN: 1, 2.14, 3 FFC: 1, 4.1, 4.4, 6