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 19-186 **August 2019, Issue #7**

BusinesSafe Threat Topic: Insider Threat

September is National Insider Threat Awareness Month! Participating in Insider Threat Awareness Month can help businesses mitigate threats and protect their communities. Businesses can participate in awareness activities through insider threat education and training programs like those listed below.

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.

- A study conducted by Verizon in 2018 found that 58% of data breaches in the healthcare industry involved insiders. Reporting indicates that most of these incidents were driven by personal financial gain.
  New Report Puts Healthcare Cybersecurity Back Under the Microscope
- In 2017, the investigation into Target's 2013 security breach revealed that the incident was likely caused by the theft of third-party vendor information. This vendor entity had external access to Target's networks likely in order to remotely troubleshoot glitches or connectivity issues. This incident highlights the importance of cordoning off sensitive networks and databases from third-party entities.
  Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned
- In 2017, a former employee of Coca-Cola stole a company external hard drive thus compromising some personally identifiable information of 8,000 employees. The company only became aware of the breach after law enforcement notified them the subject was found in possession of the hard drive.
  No Smiles for Coca-Cola After Data Breach

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, HSEC-6, FSIN 1.1, FSIN 1.6, FSIN 1.10

The Department of Homeland Security's Insider Threat Mitigation Program encourages 4 steps to protect entities from insider threat.

1. Establish a Program – Creating an insider threat program before an incident occurs may help in detecting and mitigating an incident.
2. Protect Assets – Protecting critical assets may reduce the impact of an insider threat incident. Ways to protect assets include cordoning off vital data, limiting privileged users, and removing user access when terminated.
3. Recognize and Report – Training employees in recognizing the signs of an insider threat can help in preventing an incident. Incorporating both intentional and unintentional insider threat training may be useful in spreading awareness of the threat.
4. Assess and Respond – Analyzing suspicious behavior and responding to incidents may be an interdepartmental task involving human resources, information technology/security, and legal resources.

The following Office of the Director of National Intelligence report provides recommended best practices from protecting against insider threat.
National Insider Threat Task Force: Protect Your Organizations from the Inside Out (PDF)

The following brochure, produced by the Federal Bureau of Investigation, provides an introduction to detecting and mitigating insider threats.
The Insider Threat Brochure (PDF)

To sign up to receive BusinesSafe directly to your email, visit our website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, HSEC-6, FSIN 1.1, FSIN 1.6, FSIN 1.10