




Insider Risk

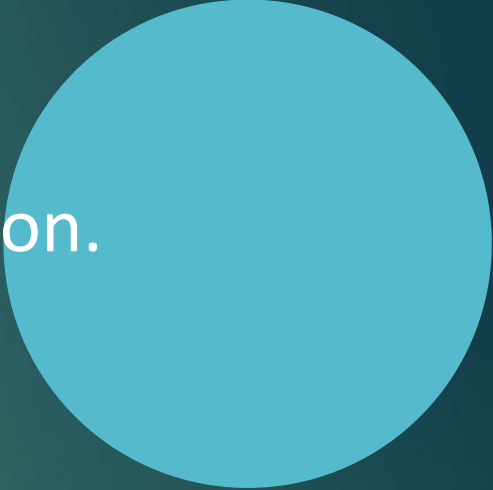
HOW VULNERABLE IS YOUR ORGANIZATION?





Why is it important to know your insider risk vulnerability?


The information that you collect is vital, important, and sensitive to your organization. Every day the information you collect is threatened by employees who can be exploited, careless, or malicious.



Question



As County Collectors, Treasurers and Finance Officers, what is the type of vital, important, and sensitive information that you collect and must protect?



Who can be an Insider?

An insider can be a trusted employee who will use internal position, knowledge, and/or authorized access to purposely or unintentionally do harm to their organization.

Insider Risk

What are examples of a trusted employee?



Types of Insiders



There three types of insiders, can you name



Careless Insiders



Careless Insiders do not purposely put your organization at risk. However, their risk is usually in the form of poor security habits

The Washington Post



Careless insiders are government's biggest cybersecurity threat

Exploited Insiders



Exploited Insiders are tricked into divulging sensitive information or allowing unauthorized access to information systems or unauthorized access to facilities.

Florida attorney general warns of tax phishing attack

Beware of conversation hijacking scams, Attorney General Ashley Moody says

Posted: 5:54 PM, February 12, 2019

Updated: 6:10 PM, February 12, 2019



Malicious Insiders



Malicious Insiders are intentional in their efforts to cause harm

One in 50 employees could be a malicious insider



By [Sead Fadilpašić](#) | Published 2 years ago

4 Comments

Like 0

Share

Google+ Tweet



How you can be targeted?

Social engineering is the most common method for manipulating an Insider. It can take many forms, such as phishing emails, phone calls, in-person contact, texting, and even connection request on social media.

Phishing

Criminals masquerade as an individual or trusted organization and use email to gain access to sensitive information or to distribute malicious software. (Most widely used and successful exploitation method today).

Social Media

Cybercriminals mask their identity in social media to connect with employees, exploiting information that is shared online.

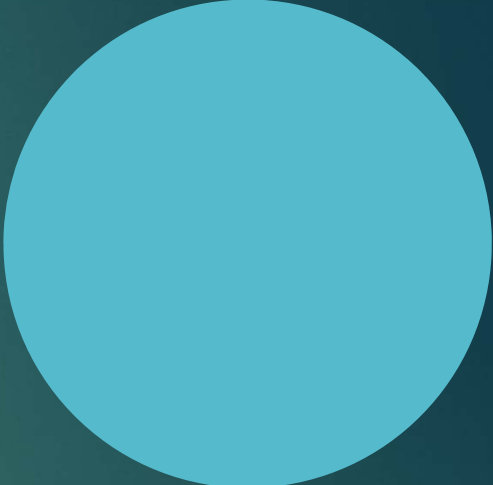


Recruitment and Exploitation

State sponsored actors or criminals use situations such as low job satisfaction, financial struggles, etc., to try to manipulate and exploit a trusted employee into helping them gain access or information about your organization.

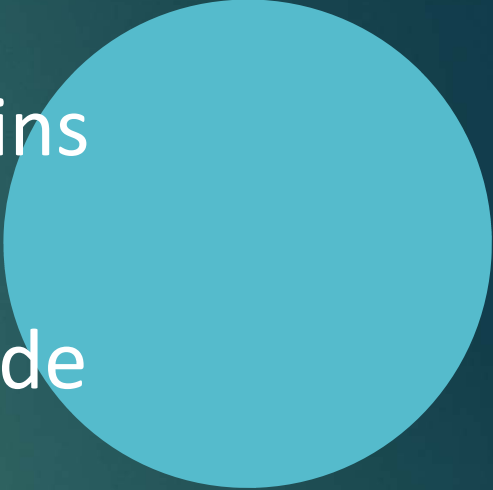
Recognizing Insider Threats



- Inappropriate Interest or Acquisition
 - Unauthorized or Unusual Computer Use
 - Unusual Hours, Contacts, or Travel
 - Secretive or Peculiar Behavior
 - Personal or Financial Issues
 - Workplace Aggressive Behavior Indicators
- 

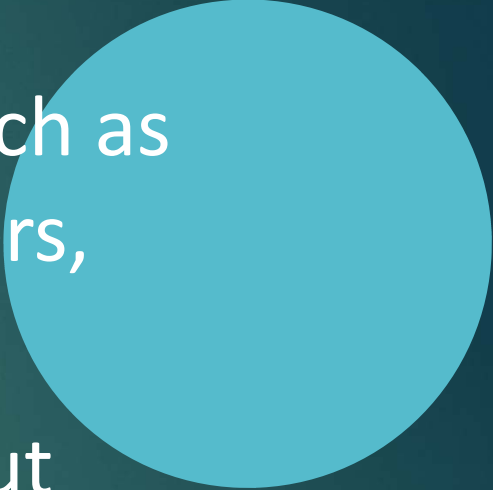
Inappropriate Interest or Acquisition



- Inappropriately seeks and/or obtains access to unauthorized locations
 - Expresses interest in matters outside scope of duties
 - Unnecessarily copies documents and information
- 

Unauthorized or Unusual Computer Use



- Exhibits unusual computer use, such as making unexplainable data transfers, etc.
 - Attempts to access systems without authorized access
- 

Unusual Hours, Contacts, or Travel



- Works odd hours without valid reasons or authorization
- Makes frequent trips to foreign countries without reasonable explanation while requesting to take organization equipment

Secretive or Peculiar Behavior



- Exhibits concerning behaviors or comments indicating intent to harm the organization, employees, or systems
- Exhibits changes in work habits such as a decrease in performance, repeated policy violations, etc.
- Loses devices frequently
- Unusual changes in behavior upon return from travel

Personal or Financial Issues



- Expresses excessive dissatisfaction with job or disloyalty to the organization
- Exhibits significant personal problems

Workplace Aggressive Behavior



- Exaggerated emotional response to what the situation requires
- Verbal threats to cause physical harm to equipment or others
- Resolving conflict by physical means or excessive verbal means
- Preputial victim mentality or unjustified perception of being put upon by others