LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

SEPTEMBER 2023

INSIDER THREAT

LIS Solutions September 2023 Monthly Newsletter topic is Insider Threat. "DoD Directive 5205.16 defines an 'insider' as: Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD. This can include employees, former employees, consultants, and anyone with access."

Without notice, an individual could have the intention of betraying their country. This betrayal could manifest through causing harm to their colleagues at their workplace, or at worse, compromising national security. Research has consistently demonstrated that insider threats often stem from trusted individuals who gradually evolve into engaging in malicious acts. Typically, these individuals are driven by personal crises or overwhelming circumstances that they struggle to overcome. If these stressors are not effectively addressed in a healthy and adaptable manner, they can lead an individual to commit acts of espionage, divulge sensitive information, perpetrate targeted violence, or inflict harm upon themselves. While employees may be deemed reliable custodians of classified or proprietary data, it is essential to recognize that they could become an insider threat.

Many times, people are hesitant to report suspicious or unfavorable behavior to their supervisor or security personnel. This can stem from not wanting to be intrusive about their coworkers lives or risk making false accusations or defamations. It is completely natural to want to give people the "benefit of the doubt." This is especially true when it's someone in a position of authority, a colleague, or a friend.

As an LIS Solutions employee, it is your responsibility to report suspicious behavior to your LIS Security Professionals at **security@lissol.com**. There are many reportable behavioral indicators that you can rely on to identify an insider threat. Previous known insiders have been affiliated with one or more of the following reportable behavioral indicators including:

- Changes in personality, behavior, or work habits.
- Substance abuse or addictive behaviors such as: alcohol or drug abuse and gambling.
- Considerable financial change such as unexplained affluence or excessive debt.
- Disgruntlement to the point of wanting to retaliate.
- Disregard for security procedures and protocols.
- Seeking access to classified or proprietary information and systems/technology without a "need-to-know."
- Access to facilities or proprietary information outside of normal work hours.
- Unauthorized removal, or unnecessary copying or hoarding of classified or proprietary material.

At your convenience, please read: Toulas, B. (2023, May 23). ***IT employee impersonates ransomware gang to extort employer.***

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

CYBER INSIDER THREATS

Cyber Insider Threats can be caused on purpose by employees who may do so through fraud or selling trade secrets or other confidential information. They may work alone or with outside entities. Insiders may be recruited by cyber criminals (including those utilized by business competitors) or act on their own. Insiders such as staff or contractors with access to confidential information may sell it to gain additional income, or to commit sabotage to harm the organization due to perceived slights by the organization.

These types of insider threats can be caused unintentionally by negligent staff. The exposure they cause may be due to lack of proper security training, carelessness, or intentionally ignoring security policies. This exposure can take the form of not securing a building or office entrance point, losing electronic devices containing sensitive data, leaving their computers physically unsecured or leaving them unattended while logged into the computer/network, not installing required computer system patches, not following policies/procedures because they are inconvenient, etc.

Cyber Insider Threats can be caused by accident. Even the most diligent employee may make a mistake such as accidentally selecting the wrong recipient to an email, inadvertently clicking on a hyperlink in an email or Web site that opens an infected file or site, or opening an attachment that contains a virus. They can also dispose of sensitive physical or electronic documents improperly so that they can be recovered by someone wanting to cause harm. An organization can't completely stop accidents from happening, but they can minimize accidents and with good communication when an accident happens, the effects may be able to be minimized.

To keep an organization, its staff, and clients as safe as possible from threats, no matter what form they take, be they Insider, External, Cyber, physical, purposeful, or accidental, a "culture of care" must be developed by the organization and actively and conscientiously followed by all staff at all levels.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com