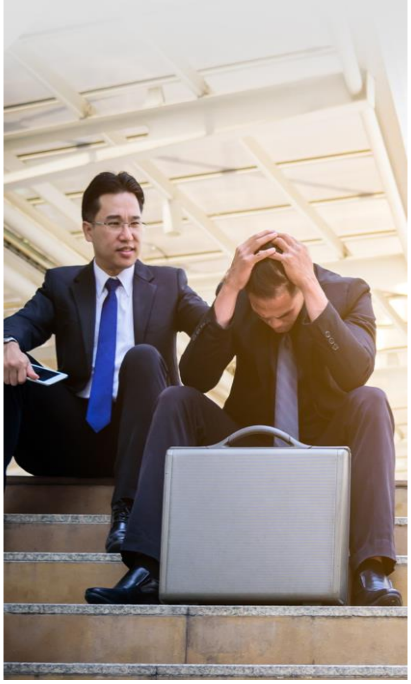
INSIDER THREAT PROGRAM

True Stories from the Inside

Turning people around, not turning them in!

Watch Out for Spills!



Insider Threat programs examine concerning behaviors with a multidisciplinary team to deter, detect, and mitigate risks associated with insiders. This proactive strategy often identifies and resolves issues before a potential insider becomes a threat to themselves or protected resources, such as personnel, information, and property. Insider Threat programs can only address these behaviors if they are reported. Many of us feel conflicted about reporting concerning behavior and worry we'll cause problems "over nothing." However, it's essential that all concerning behavior be reported. If it's nothing, no action will be taken. In cases of increased risk, Insider Threat programs have an opportunity for intervention prior to any negative event. The goal is to protect our warfighters, our nation, and its secrets.

The following events are based on a true story.

A U.S. Government agency recently identified several instances of improper handling of classified information. Some employees were failing to properly follow file transfer procedures. In this case, transfers to portable storage discs, such as CDs and DVDs, were not being adhered to. This negligence increased the possibility of a data spill potentially leading to the unauthorized disclosure of classified information.

A data spill occurs when classified data is introduced to a system authorized at a lower classification, or to portable storage media. Regardless of how the data spill occurs, it has the potential to cause grave damage.

Whether intended or inadvertent, insider data spills increase risk within organizations. They also require an Administrative Inquiry to report the spill, assess the risk, contain and clean up the spill, and preserve all evidence for any required investigation. Remember, only cleared personnel may conduct cleanup actions and quarantine impacted systems and peripherals.

Another spill?

Another potential source of spills the agency identified occurred because employees were not properly classifying e-mails. Improper classification can lead to unauthorized disclosures. In one example, an employee received an e-mail on SIPRNet that was classified. The employee wrote an unclassified response but failed to properly classify the message based on the entire e-mail thread.

How did the agency respond?

The organization initiated an appropriate incident response, including containment and clean-up. However, the bigger issue to be addressed was preventing spills in the future. The agency created targeted training to make sure employees knew the proper data handling procedures, including transferring data properly and handling data spills appropriately. The agency's mitigation response to both the individual issues and larger organizational mitigation strategies resulted in reduced risk.

For more information on the subject of data spills and proper file transfer, check out two short eLearning courses from CDSE:

Assured File Transfer

Data Spills

For more information on derivative classification, check out CDSE's eLearning course:

Derivative Classification IF103.16