Webinar Questions and Answers

DSS Cyber Insider Threat

Webinar guests submitted several questions before and during the April 10, 2014 DSS Cyber Insider Threat session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: Who is required to have a program? What exactly is the requirement for Industry?

Answer: For federal agencies, White House Memorandum dated 11/27/2012 "Handling Guidance for the National Insider Threat policy and Minimum Standards" under EO13587, requires the establishment of an insider threat program. At this time, there is no NISP requirement for industry to establish an insider threat program. However, conforming change to NISPOM expected in FY15 will likely have insider threat program requirements.

Question: Can you provide examples of reportable CI events?

Answer: In addition to DoDD 5240.06, please see CDSE publications: http://www.dss.mil/documents/ci/Reporting-the-Threat.pdf, http://www.dss.mil/documents/ci/Insider-Threats.pdf.

Question: Which industry best practices or strategies can lower-level Information Assurance practitioners use to best mitigate this threat?

Answer: Following the best practices suggested in our downloadable handouts and employing a multi-disciplinary approach can be very effective in detecting, deterring, and neutralizing the cyber insider threat.

Question: What are the signs and what can you do to counter them?

Answer: Technical and behavioral indicators are prevalent in most instances of Cyber Insider Threat. Early reporting of these indicators to appropriate security, IT, and CI personnel is an effective countermeasure.

Question: We are a possessing defense contractor. Please review instances of cyber insider threats for non-possessing facilities.

Answer: As noted in the webinar, cyber insider threat encompasses more than just the spy. Instances of fraud, theft, and sabotage are equally prevalent and can damage companies, economy, and national security. For more information on cyber insider threat cases, visit the DHS and FBI Cyber Insider Threat websites identified below.

Question: How can we protect information when it is so easy to insert a flash drive into the computer?

Answer: Consider your company and organizational policies regarding the use of removable media. There is also the concept of "Tag the data, tag the people." Connecting data with the people who have the appropriate clearances to access to the data, can serve as a tracer to identify who may have inappropriately released information. Which can also be an effective deterrent.

Question: What is the primary vehicle used by most organizations to detect IT threat?

Answer: Most threats exhibit behavioral and technical indicators and can be observed by supervisors, coworkers, and technical audits. The most effective deterrent is to report these indicators as soon as possible.

Question: How do you get your organization's CI, IA, IT, security, and other elements to understand that combating insider threat is a shared mission?

Answer: Refer them to the webinar! In addition to following information assurance guidelines and employing technical measures designed to protect information systems, consider the roles of Personnel Security (helpful perhaps in identifying some of the personnel issues which may contribute to cyber insider threat) and Physical Security (which can impact access and other factors), as well as industrial security, foreign ownership, control and influence issues, supply chain risk mitigation, operations security, and continuity of operations planning. It is only by incorporating each of these security disciplines and through the application of a defense in depth approach, that we can begin to mitigate our risk by limiting access, increasing reporting and detection, honing our responses, and employing effective deterrents.

Question: How does an organization work to identify observable and reportable external cyber threats that may be linked to internal cyber insider threat activities?

Answer: By reporting all illicit cyber activities, IT, Security, and CI components can appropriately conduct inquiries and/or investigations to determine the nature and complexity of the threat.

Question: What sort of lower level tests can lower level IAOs conduct that won't land them in jail?

Answer: CDSE does not recommend that you conduct extralegal operational training activities. Work with your security staff and legal department to determine if any training or testing is within the guidelines of your organizations policies and the law.

Question: Is there a resource available to view releasable details of actual threats so we can better look for them in our own areas?

Answer: Please review the DSS Counterintelligence Reports at http://www.dss.mil/isp/count_intell/ci_reports.html. In addition, DHS US CERT and FBI both publish information on cyber insider threat at http://www.fbi.gov/news/stories/story-index/cyber-crimes OR https://www.cert.org/insider-threat/