CyberPsychology: Conquering Insider Threat

The greatest cybersecurity risks your organization faces are breaches due to accidental, negligent or malicious activities of an organizational insider. Together these represent the largest risk of financial loss and reputational damage to any organization. In this crucial session attendees (IT and non-IT experts) will learn how to develop an organizational approach to insider threats and how to implement proactive approaches to recognize evolving risks and weaknesses. Attendees will learn the important assets they can use to detect and thwart security risks. They will understand breach tactics, behavioral and data patterns that indicate risks, and the most effective weapons against insider threats in the ongoing cyberwar.

Major Subjects:

- Breach Tactics
  - Exploiting control gaps and control weaknesses
  - A review of tactics by type of attack
  - Psychological tactics used in attacks
- Closing the gaps
  - A review of robust controls
  - A review of the audit, HR, IT and management relationships
  - Proactive approaches to recognize evolving risks and avoid breaches
- Developing an effective insider threat program
  - Program transparency
  - Useful assets to recognize and thwart risks
  - Intra-organizational support and coordination

Learning objectives: Attendees will learn about breach tactics, effective controls, and how to develop an insider threat program. They will understand the assets and coordination necessary to implement an effective and adaptable defense.

Level: Basic
Prerequisites: None
Advanced preparation: Not required

Hours: 1-4. Session available in 1-2 hour keynote format, a 1-2 hour presentation format or 2-4 hour workshop format.

Designed for: Analysts, auditors, governance and compliance professionals, and those working in the IT, HR, legal, and medical professions as well as executives, policymakers and other decision makers interested in developing and effective insider threat cybersecurity program.