MATURING AN INSIDER THREAT PROGRAM

Executive Order 13587, signed October 7th 2011 by President Obama, set to correct massive vulnerabilities highlighted by Army PFC Bradley Manning. Manning was a young Army solider that while deployed burned hundreds of thousands of classified documents to a disc and simply walked out. The information that he stole was then given to Wiki-Leaks and other media partners to "inform the public".

The purpose of E.O. 13587 is to "Detect, Deter, and Mitigate" an Insider Threat. Standing up a program capable of detecting an insider is an intricate process to include almost every aspect of any agency, company, or enterprise. Collaboration among all parties is key to developing an effective program, however getting all parties on board with an Insider Threat program is very difficult. Due to the title of "Insider Threat", most employees see it as a way to spy on employees or that the agency doesn't trust the employees. This stigma requires a delicate but firm approach by a knowledgeable Insider Threat representative.

Building an effective Insider Threat program can be expedited by having a qualified staff that is able to be the liaison between all parts of the program. Having a focal point that can identify the legal lines but also able to write effective policies and rules for a User Behavior Analytical (UBA) tool will set your Insider Threat Program leaps and bounds over any other program.

One of the most overlooked steps in an Insider Threat Program is the deep evaluation of current vulnerabilities or current threats. Identifying major vulnerable areas within an organization can be accomplished by simply communicating with employees. Employees are in their

respective areas on a daily basis and will notice issues of safety and security. They are one of the most important resources for any Insider threat Program, therefore getting them involved in the beginning is considered a best practice. Identifying areas that don't have proper security controls such as cameras, locks, or have direct access to sensitive areas are in most cases an easy fix.

Insider Threat Programs can be extremely complex, however taking the simple not so obvious steps can expedite the entire process. Employees are the eyes of the agency, they are one of the most valuable resources to not only the agency but also the Insider Threat Program. Educating them on the process, risks, signs, and potential damage can make or break a program. Consider them the off-line UBA tool.

Contact Us: Alex Wang, Chief Operating Officer / alex.wang@markesman.com • 609.558.2898

MATURING AN INSIDER THREAT PROGRAM

Areas for Maturing an Insider Threat Program:

+ Policies, Procedures, Tactics, and Rules of Engagement
+ Employee Education and Management Buy-in
+ Technical Controls & Tools
+ Incorporation of all parts of the agency, HR, Cyber, Personnel Security, Physical Security
+ Collaboration and tuning available data sources
+ Identify Risks, Vulnerabilities, and Current Threats
+ Segregation of Insider Threat information for Confidentiality

These areas of any Insider Threat Program need to be well understood to stand up and maintain the program. Having a dedicated team of Insider Threat Experts is unplausible due to budget restraints, which further emphasizes the need for a single representative that can work, manage, and create the needed relationships. Selecting an individual that can be a solid asset needs to be viewed from an overall program. With cyber being one of the most intensive parts of a program, selecting a cyber-representative, dedicates a cyber-member for the most in-depth parts of the program. With a DoD 8570 qualified representative an agency has a Cleared and Certified member to meet the sensitivity and cyber standards needed. This member becomes the focal point and go-to Insider Threat representative that can work with Employees and Upper Management with Insider Threat as #1 priority.

MARKESMAN GROUP

Markesman LLC is able to provide Cleared, Qualified, Trained, and Experienced Insider Threat Staff. Having been trained by the National insider Threat Task Force under direction of the Director of National Intelligence, Markesman provides the needed expertise for such a delicate program.

Recent Most Detrimental Insider Threat Cases

ALL WERE TRUSTED INSIDERS

Reality Winner

NSA Contractor

+ *Allegedly* gave TS Document to News Site for Personal Reasons

Edward Snowden

NSA Contractor

+ Leaked 1.7 Million DoD Files to include TS SCI Documents
+ Fled to Russia

Bradley Manning

US Army

+ Leaked over 490,000 Classified Documents
+ Sentenced to 35 Years, Served under 4 years

Contact Us: Alex Wang, Chief Operating Officer / alex.wang@markesman.com • 609.558.2898