How to Conduct an Insider Threat Investigation

San Diego ISAC Counterintelligence Sub-Committee – August 2018

Setting the Stage; Or, Experience Required?

A popular misconception regarding investigations revolves around individual capability. It is important to recognize an Industrial Security Insider Threat investigation does not require the investigator to be Sherlock Holmes with deerstalker hat on head and curved pipe in mouth nor does the investigator need to have memorized the U.S. Army Field Manual (FM) 34-52 *Intelligence Interrogation*. An Insider Threat investigation is neither a shocking murder mystery nor is the investigation conducted on the battlefield; so, proceed with the understanding the investigation will occur in the business environment involving the interviews of coworkers. An investigation should be approached in a methodological manner, step-by-step, wherein the investigator collects all available information towards considering individual culpability as well as whether or not sensitive information or materials have been compromised.

Receipt of an Insider Threat Allegation

Each and every single Insider Threat investigation begins with an allegation; therefore, the allegation is the foundation upon which the investigation house is built. Where did the allegation originate? Perhaps an employee submitted an anonymous tip by means of the company Open Line. Or, possibly specific data logs were identified by Information Technology showing an abnormal amount of email messages sent to both personal email and competitor-based email addresses. All allegations must be taken seriously from the onset regardless of source. The source itself must also be considered and weighted for reason there is a great divide between established company resources fulfilling a statement of work versus what could be a biased complaint stemming from a personal grudge. If at all possible, the investigator should conduct the first interview with the source in order to determine if any additional details can be learned about the allegation. The source may have left out important facts when filing; perhaps the source was limited by a reporting process involving an online form of 2,500 characters or less. By engaging the source, the practice of telling the story out loud may prompt additional memories of the event.

Policies and Procedures

An investigator absolutely must be knowledgeable of company policies and procedures, not just the single document drafted to show the Defense Security Service (DSS), or any other customer entity, how the company fulfills Insider Threat Program requirements. Policies and procedures set the framework for employee behavioral and work-based performance expectations; policies and procedures will also define and set protection measures for what types of information and materials are deemed proprietary. An Insider Threat allegation involving an employee storing proprietary information on a personal phone or laptop is baseless if the company does not maintain a standard for protection of information which addresses Information Technology asset requirements for company and personal devices. Knowing company policies and procedures will enable the investigator to engage both the subject of the allegation as well as additional interested parties from a position of authority.

Additional Interested Parties?

An Insider Threat investigator is not a team by him/herself. Of course, Industrial Security will have valuable records for reference including training records, foreign travel/contact reports, and possibly even incident or adverse reports. An Insider Threat investigation is given purpose and greater depth when disciplines beyond Industrial Security are consulted. While still in the pre-subject interview phase the investigator should consult with the subject's Manager, who should be able to clarify the subject's current tasking and possibly even detail in depth how the tasking should be completed. A Manager should know if an employee is using USB portable hard drives to transfer gigabytes of data between network devices at 1:30am. Human Resources is an excellent source of information related to behavior. Human Resources can identify if the subject has received sub-par performance ratings or discipline related to instances where the company's code of conduct and expectations were not met. Perhaps Facilities manages access control and closed circuit television recordings and can provide additional evidence related to the allegation. As mentioned earlier, Information Technology can be the Most Valuable Player when providing activity event logs related to the timing and other details of emails, websites, print jobs, and device connections. Legal Counsel also plays a large role on the team, possibly due to the need to delineate boundaries and provide oversight to the investigator and team working towards the best possible outcome for the company as a whole. Oftentimes Insider Threat investigations push into the realm of privacy, and Legal Counsel serves to clarify proper interpretations of laws beyond company written policies and procedures.

Fully Prepared

A sizeable amount of information should already be held by the investigator before contacting the subject for interview. It does the investigator good to take the time to draft an outline, to set in order everything gathered since the receipt of the allegation. The outline will aid the investigator in identifying key points which need to be discussed with the subject. Additionally, the outline can be supplemented with notes taken during the interview and can serve to establish an order for the interview; an investigation interview can often swerve in varying directions depending upon the subject and the environment the interview takes place in. Before contacting the subject for interview the investigator should already have identified a time and location for the interview. While scheduled time can be flexible based upon work requirements, it is recommended the location of the interview take place free from distraction; a conference room or office away from the subject's normal work station serves multiple purposes of limiting

interruptions, allowing for focus, as well as reduces the potential embarrassment of being the subject of investigation.

Direct and Open-Ended Questions

Having finally arrived at sitting face-to-face with the subject, the interview can begin. It is likely the subject of the allegation will be anxious and can quickly turn defensive if the investigator pushes the situation in such a direction. It is possible to begin the interview with basic background and employment questions simply to set a comfortable tone; questions regarding date and position of employment establish a question-answer relationship with irrefutable answers and can be followed up with details regarding statement of work. For example, the subject has worked on site as a software engineer since May 2015 and currently is part of the team developing algorithms for redundant communication links. The discussion can easily transition into identifying the subject's work schedule and location details. The investigator should always utilize direct and open-ended questions which prompt the subject to provide details and should never simply be answered in a 'yes' or 'no' fashion. For the investigator to ask indirect and closed-ended questions is erringly guiding the course of the discussion, steering towards an already assumed verdict. No one can deny there is a vast difference between "Did you arrive at work on Monday at 10:15am?" when compared to "When did you arrive at work on Monday morning?" Although the answer may still be 10:15am, the investigator now has the opportunity to follow up with "Why at 10:15am when the normal working day schedule starts at 8:00am?" or some similar interrogative.

Interrogatives

Revert back the basics of who, what, where, when, why, and how in order to prompt a storyline from the subject. These basics will enable the investigator to understand the validity of the allegation from the subject's point of view. Although an outline was suggested as part of preparation the investigator should not be limited to the outline like a rigid checklist. The investigator has to be flexible enough to continue pulling on threads, asking the "who else" until no one else is identified, asking the "what else" until nothing else remains to be acknowledged, etc. Working a specific item through to its logical end can be especially challenging when considering the varying forms information takes and where it can possibly be transferred to. If a document was printed into hard copy, then where was the hard copy stored, were copies made, and was it rescanned then emailed or uploaded into the cloud? If an unauthorized USB hard drive is connected to a company asset then necessary follow up questions involve who had access to the hard drive since transfer, what other devices was the hard drive connected to, and did further transfer of the files to the additional devices take place?

Objective

The purpose of the interview is to determine culpability and compromise, and the investigator may need to address these during the subject interview. It is not recommended the investigator either begin or turn an interview by preaching policy and procedure. Instead, the investigator should ask the subject his or her understanding of company policy when the line of questions and answers have arrived at the substance of the allegation. It is here the subject will either recognize and admit wrongdoing or feign ignorance. If the latter, then the investigator has the opportunity to further present evidence collected during the preparation phase. The subject will find it difficult to deny the raw data of badge swipe or email activity, which is just as irrefutable

as being employed as a software engineer since May 2015. Hopefully not all Insider Threat investigations are Industrial Security thrillers; it is truly best case scenario if an Insider Threat investigation arrives at the fortunate conclusion of a misunderstanding with no culpability or compromise. However, if culpability or compromise is identified then the investigator should follow through with the appropriate next steps.

Recovery

There is a certain degree of fear of the unknown with having been identified as culpable for an incident. Hopefully most employees who commit a security incident only do so once, meaning the individual has learned his/her lesson as appropriate. Since most individuals are not repeat offenders there is the void of what comes next. The investigator should take the opportunity to clearly define expectations as well as schedule of what lies ahead. If the Insider Threat investigation involves an unauthorized portable hard drive, then the investigator should clearly impress upon the culpable employee the need to retrieve the portable hard drive and surrender it immediately in an as-is state without connecting the portable hard drive to any additional devices. The investigator should also have readily available a Surrender of Personal Property form approved by Legal Counsel which states the company will be conducting forensics review on the device for purposes of the investigation. The culpable individual should be advised of the reporting process wherein the investigator will fully document the matter for record, to include giving the culpable individual an opportunity to submit a written and signed statement of interview; a statement serves the purpose of inserting the culpable individual's point-of-view into the report of investigation and adds a degree of separation and objectivity to the investigator's report.

Conclusion

Just like riding a bike, investigations take practice. The more investigations an investigator conducts the better he/she builds relationships with needed disciplines as well as becomes adept at exercising the question-answer back and forth while fleshing out details to their fullest extent. Insider Threat investigations are dynamic and challenging for all involved, but even more so for the investigator who serves as the first responder on site for the incident by engaging with the alleged culpable individual. Just as important as conducting a thorough investigation is the matter of writing a thorough report. Please look forward to the next article to be presented by the San Diego Industrial Security Awareness Council Counterintelligence Subcommittee addressing how to write an investigation report.