011614 Webinar

Insider Threat Brief

Today's conference is being recorded, if you have any objections you may disconnect at this time. The host for today's call is Mr. Peter DeCesare, thank you and you may begin.

Pete: Good afternoon! Welcome to the CDSE Learn at Lunch webinar. Today's topic is Insider Threat. I am Peter DeCesare, the Counterintelligence Curriculum Manager here at CDSE. Linda Adams is our production manager today. Linda please take a few minutes to explain how the DCO webinar works.

Linda: Thanks Pete! Before we get started let's take a tour of our DCO meeting room. In the bottom left hand corner that's marked with a green arrow here, you'll find a notes box. This lists the call in number and other announcements. If you are disconnected from the audio, this number will remain on screen for your reference. Also on the screen you'll see our notes regarding using full screen. If you look at the gray banner on top of your screen, you'll find the full screen option there. However, when poll questions appear, select full screen again to return to normal view and respond to the polls. You'll find a file share box in the location indicated by the yellow arrow. Here if you select a file the save to my computer button will highlight and you can download this file which is the pdf of the slides to your computer. It's the same thing that was sent out earlier in your welcome email. You'll also find a Q&A box for entering questions to the presenters. This is marked here with a blue arrow and it's on the right side of the screen. To communicate with us, simply type your question into the box as shown. Any questions and answers that are not covered during the webinar will be posted to the website. During this webinar, we will be asking two types of poll questions. For open answer poll questions all you have to do is type your answer in the chat box that will appear on the right of the screen. Don't forget to click the full screen again if you have been viewing in that mode, or you will not see the poll question. The other poll question will provide multiple choice answers for you to respond to and all you have to do is choose what you believe to be the best answer and we'll provide you feedback. Don't forget again to click on the full screen if you've been viewing in that mode or you won't see the poll question. Okay Pete that about covers the technical part so back to you.

Pete: Thank you Linda! Before we get started, please be aware that the video portion of this webinar is being recorded. Once the red recording light appears, we will begin. The counterintelligence folks have been giving threat briefings for years, advising the community about the foreign intelligence threat and telling spy stories about some of our more infamous espionage cases from Benedict Arnold to John Walker, Rick Ames, Bob Hanson and many others. Recently however, we have become more focused on the Insider Threat. Following the Ft. Hood shooting, Wiki Leaks, NSA's "Whistle Blower" Eric Snowden, and the most recent Navy Yard shooting, the community is feverously reacting to the Insider Threat. In November 2013, the President signed a memorandum which requires all agencies to establish an Insider Threat Program to help deter, detect and mitigate the potential insider threat to help protect our nation's classified information. In the near future, we expect a conforming change to the NISPOM which will also include language to incorporate insider threat program requirements for protecting classified information possessed within our cleared contractors.

Our guest speaker today is Nicole Haager. Nicole has been an Intelligence Operations Specialist within the Counterespionage Division of the DSS CI Directorate for four years. A former U.S. Army CI Special Agent, Iraqi veteran, and investigator, Ms. Haager has a vast experience as an Intelligence Operations Specialist, collector and analyst. Welcome Nicole!

Nicole: Thank you Pete! Today we are going to discuss the Insider Threat.

- What is Insider Threat?
- Why is the Insider Threat significant?
- How do you recognize the Insider Threat?
- How can you help defeat the Insider Threat?

From a CI perspective, the Insider Threat is an employee with access to a classified or controlled environment who has the opportunity, capability, and intent to purposefully compromise sensitive information and/or materials for distribution to entities who pose a risk to the security interests of the United States. Next slide please!

Linda: Okay Nicole, here's our first poll for everyone, this will be a fill in the blank.

Question: Specifically what types of information are at risk due to Insider Threats?

So you can just type into the blanks at the bottom of the chat box and we got some folks responding. Oh great, we have classified and proprietary, intellectual property, everything, PII, sensitive information, CUI, SBU (I'm not sure what that stands for), classified, classified PII, sensitive but unclassified, proprietary infrastructure, OPSEC, export control, loss of life, sensitive but unclassified (oh I see that is SBU, thank you), COMSEC, FOUO, PII classified export control. Okay we're starting to get some repeats here. COMSEC, ITAR, prep info, information technology, weapons, SBI. They're slowing down here, violence, unfortunate demise of life, network access, wow all kinds of things. Alright, so how did they do Nicole?

Nicole: And I believe that everyone is pretty much hit on everything we have here on the slide. Now the threat posed by Insider activity in support of foreign powers, criminal enterprises, and terrorist groups has the potential to endanger lives, compromise resources, and significantly diminish our capacity to effectively execute our mission. So, as you can see Insider Threat has a substantial impact on National Security and industry. Next slide please!

Globalization poses new challenges with the increase of dual or multiple citizenships and country of origin cards which allow persons to travel to issuing country without first obtaining a visa. This, unfortunately, could result in diluted or conflicting allegiances. Next slide please!

However changing business environment definitely affects the threat of insider activity with layoffs and downsizing, furloughs, sequestration, transferring jobs overseas, all of which could contribute to our workforce losing obligations of loyalty in the workforce, which may in turn diminish the expectation of loyalties to the nation. Next slide please!

Industry has increasingly become more vulnerable to insider threats due to the increased access to sensitive information. Snowden and Manning are excellent examples of cases where, maybe their access should have been restricted to the programs or duties for which they were assigned. Also frequent travel, conflicting national loyalties, the vulnerabilities created by all of these trends increase the risk of Insider Activity. Next slide please!

Linda: Alright here we have our next poll Nicole.

Question: What are some of the more common PEIs or Potential Espionage Indicators? Let me grab the chat box over here so everyone can give us your answers, we've got some responses coming in. Let's see we have security violations, late night working, odd hours, working late, lots of foreign travel, after hours, bad economic status, foreign travel, extra hours, dual citizenship, inappropriate excessive questions, increase of financial obligations, financial trouble, unannounced foreign travel, gambling problems, (we didn't see that one this morning), extra money travel, weird hours, repeated security violations, requesting access to a program, request for greater access, late hours, affluent odd hours, divorce, high risk, unexplained increase in money, excessive time off, alcoholism, international web activity. We got some different ones this afternoon. Alright let's see how they did. And our next slide says: Exploitable behavior, we didn't see that this morning that was good to see this time around and I believe we're all familiar with the list of PEIs that are commonly noticeable in cases where a trusted employee has engaged in espionage. I would like to add to this list undue affluence, disgruntlement, mental instability, and another that I will explain bit and I think that while one person did touch on this a bit, when with the absence of financial hardships when in certain situations you might expect for a person to have some sort of financial problems for example: A person who's going through a divorce, and maybe paying for a separate home, child support, spousal support etc, and that person never seems to complain about their finances. Instead it's business as usual or maybe they're still spending money or buying another car, so those could also be indicators.

Not to say that every person who exhibits one or more of these indicators is involved with illicit behavior, but most of the persons who have been involved in Insider activity in the past were later found to have displayed at least some of these indicators although their former co-workers and supervisors rarely felt compelled to report this behavior to the proper authorities. Next slide please!

Linda: Alright our next poll is to ask the folks if they can define Anomaly? And here's your chat box so let's see what we get. We get deviation, exception, oddity, something unusual, strange occurrence, out of the ordinary, something odd or out of place, abnormal, when a foreign company has access to something they shouldn't have, different from the norm, not the standard, (this group is hitting the nail on the head), bizarre, variance, questionable (that's a good one too). Alright I'll leave that there for second and come over here. There's the definition for anomaly.

Nicole: Anomaly is a situation where a foreign intelligence entity appears to have knowledge or possession of information they are not expected to have. An example would be the appearance of classified or proprietary design features of US weapon, or communication systems and you see that in comparable systems produced by a foreign defense industry, our space shuttles, our helicopters, satellites, all of those are great examples of anomalies. Next slide please!

Trends of individuals who have committed espionage:

- 1/3 of spies are naturalized U.S. citizens
- More than 1/3 of spies had no security clearance
- Twice as many spies volunteered as were recruited (and we've seen that with Manning and Snowden. They were just volunteers.
- Most recent spies have been solo actors
- Nearly 85% passed information before being caught
- The most recent cases, 90% used computers in their espionage, 2/3 used the internet

- 80% received not payment for their spying (Linda: I think the one that surprised me the most was that more than a 1/3 had no security clearance) Yes we're looking at proprietary information. Next slide please!

Linda: Here's our next poll question and this one actually has some answers, so we'll go ahead and select the answer that you feel is correct. Who are we trading secrets with? We have Asia, Europe, Africa, South America and Australia as our options. And it looks like it's at the moment overwhelmingly Asia. The 60% plus percent, 67%. We have about 20% Europe, we have some Australia. Alright it looks like we're settling down to just around 68-,69% for Asia. Clear winner here! Ok and the answer from you Nicole is?

Nicole: That would be Asia, very good. We have Asia, Southeast Asia, those countries. Central/South America and our former Soviet States. Great, think we're headed to motivation.

Linda: Absolutely! So what is the motivation for spying? So let me pull over our last chat box here for you folks to give us what you think the most motivation is for spying. Money, ego,(money and ego looks like the big ones here), disgruntled, grudges, unhappy, women, ideology, get back at the government, disenfranchise with government and financial, unhappy with policies, lot of disgruntlement here. Looks pretty good. (Nicole: let me see my brief before). Let's see what the right answer is.

Nicole: Number one would be focused on loyalties other than the US. Surprisingly the motivation for spying has shifted from money to divided loyalties as the number one motivation and followed by disgruntlement. Money is now last, so the motivation for spying has shifted greatly. Also due to multiple citizenships, and country of interest cards, layoffs, furloughs, all of which contribute to Insider Activity. Next slide please!

These next two slides of case studies illustrate the changing indicators in individuals arrested/convicted of spying. We have Mak, Chung, and Hasan, they all struggled with divided loyalties. And Mak and Chung it was with China, and Hassan struggled with the wars in Afghanistan and Iraq and his Islamic faith. Next slide please!

Roth and Keyser both have a lot of foreign travel, but Keyser had undisclosed foreign travel and that is a big indicator. And with Roth is was an excessive amount of foreign travel for conferences and symposiums. Next slide please!

Ok now with Snowden and Manning they were disgruntled and disillusioned with our government and current administration. So how do we mitigate this threat? So it would be on the next slide. Employees need to maintain awareness and training and most of all report suspicious behaviors and activities to your Security Manager or your FSO or your Counterintelligence element, so you must report. Next slide please!

For our Security Mangers and FSO's you need to train, and brief, and communicate accountability, policies and expectations, and enforce the established policies and procedures. Once adverse information is reported, take appropriate action, suspend access, conduct inquiries, and most of all report. And with our proposed Automated Continuous Evaluation Program of cleared individuals, this will also aide the FSO's in reporting that adverse information or suspicious activity. Also hopefully with this new continuous evaluation program, we won't be waiting 5 years, 7 years for periodic re-investigations. It will just be random polled, you'll have to just update your SF86. So then we'll know if you've gone through divorce, or if you're now in counselling, if you've had security violations and you'll start hearing this testimony from those co-workers and supervisors, just to kind of keep us all up to date and aware of what's going on with our co-workers. Next slide please!

Reporting Requirements of PEI: The DoD Directive 5240.06 is the CI awareness and reporting directive. Now this is the Enclosure 4, this covers reporting, and I'll let you read that there, what we are obligated to report. And I will, I do want to make a note that DoD personnel who fail to report information as required, may be subject to judicial or administrative action, or both, pursuant to applicable law and regulations. Next slide please!

And I don't want to leave the contractors out. Contractors also have an obligation to report suspicious activity as well. And your reporting requirements and guidelines would be found in the NISPOM, and I'll let you take a look at this slide here and read that over. Next slide please!

In conclusion "You are the First Line of Defense".

- The Insider Threat is the most damaging
- Most were authorized access in conjunction with their work assignments
- May have circumventing the need-to-know principle
- Insiders are recruited or volunteer

And I think what we're seeing right now are a lot of volunteers and also people doing it for other reasons other than money these days we're looking at disgruntled employees, and those with divided loyalties. Next slide please!

CI, Security, & Information Awareness Core Mission is to: Protect against the loss or compromise of critical U.S. classified information and technologies by preventing penetrations by Foreign Intelligence Services and detecting, deterring and mitigating the threat posed by "Insiders". This is our core mission and this is what we need to take away from this briefing report. Next slide please!

What are your questions?

Pete: Alright Nicole, before I turn some of these questions over to you, I'd like to take on a few that actually came in when folks were registering for this webinar.

Question: What is the latest guidance for Insider Threat policy for cleared contractors?

Answer: As I mentioned during my introduction, the President just signed the required Insider Threat in November 2012 and the policy makers haven't quite caught up with that yet. We expect the conforming change to the NISPOM during 2014 to include language for the Insider Threat program and it's requirements. So stay tuned that should be coming in sometime soon. A follow on to that same line of questioning is:

Question: Can an Insider Threat Program Manager and FSO be one and the same?

Answer: Again we're still waiting for that conforming change to the NISPOM, but I did see a draft and the draft language does not preclude the FSO from being designated as the Insider Threat Program Manager. What is states is the contractor will designate a U.S. citizen employee who is a Senior official and cleared in connection with the facility clearance to establish an insider threat program and be the company point of contact. So I guess a lot of it depends on company to company, obviously a smaller facility where folks wear multiple hats. You can probably bet the FSO will also be the insider threat program manager. But again we'll see when the NISPOM change does come out.

Question: Do you have guidance on establishing an Insider Threat mitigation program.

Answer: Glad you asked. As a matter of fact CDSE did put out 2 Insider Threat courses, eLearning training that just came out a few months ago. One of those establishing an insider threat program for your organization, Course number CI122.16, you can find that on STEPP, although the Insider Threat Program is not required by industry. We basically wrote that course knowing that it's coming, and that course provides pretty good outline and guide for the Insider Threat program manager to build their own program. You can add or subtract what we have there, but, we followed the minimum standard guidance that did come out with the National Policy.

Question: What should we be looking for?

Answer: I think in the soft intro we did mention upcoming webinars. And in March, actually March 13th we have "Potential Espionage Indicators or PI detection Actions Outside the Norm". Now Nicole did mention some of the PI but in March we're going to go into a little bit more depth on what to look for what should be reported. So let me turn some of these other questions over to you Nicole.

Question: Who do you report suspicious activities to?

Nicole: Well you would report suspicious activity or adverse information to your Security Manager, or FSO or your Counterintelligence element.

Question: What types or forms of protection exist for those who report suspected anomalies or actions that could lead to identifying an Insider Threat?

Nicole: Well I would refer everyone back to the DoD Directive 5240.06, which is the directive that covers Counterintelligence awareness and reporting. I suggest everyone pull it up and take a look at it online. And there's a lot of information in the Directive PEI, what you should be looking for, who you should report suspicious behavior activity to, and adverse information, who you should report that to. Also I should mention that there is no reprisal for reporting adverse information to the FSO or Security Manager or the Counterintelligence element. And that's including reporting your supervisors. So, no reprisal!

Pete: Good. As a matter of fact during your presentation you did bring up the 5240 and the Enclosure 4, which although it's not NISPOM guidance, that Enclosure 4 gives a very good checklist of what should be reported whether DoD or industry, whether it's a Foreign Intelligence entity, insider threat, a cyber-attack or a terrorist as a matter of fact. So I think we're just about out of time here, so we're going to have to cut this a little short. There's still some more questions but I want to remind our participants that we will type these things up, get them edited and post them in the archives.

So if we didn't have time to answer your question, please look forward to checking that out in the archives. And you can always go straight to your DSS IS rep or CI guy out there too. Again, outstanding presentation Nicole, thank you very much for joining us today. You all have a great day. Bye!