INSIDER THREAT TRAINING

“Insider threat” is the term used for the potential harm posed when an individual intentionally or unwittingly uses or exceeds access to negatively affect information or systems, or compromises our government customer’s mission.

Insiders committing illegal acts and unauthorized disclosure can negatively affect national security and industry in many ways. These acts can result in:

- Loss of technological advantage
- Compromise of classified, export-controlled, or proprietary information
- Economic loss; and
- Even physical harm or loss of life.

These types of threats from trusted insiders are not new, the increasing numbers of those with access to data and the ease with which information can be transmitted or stored can make illegal access and compromise easier. A recent DSS brochure on insider threats cited that in the 11 most recent cases, 90% used computers while conducting espionage and two-thirds initiated the contact via the Internet.

LOOK FOR AND REPORT INDICATORS OF POSSIBLE INSIDER THREAT

We must all be on the alert for behaviors that might be indicators of an insider threat. Knowing the safeguards that must be applied to handling company and customer information, report behaviors such as:

- Mishandling or misusing company or customer information
- Removing company or customer information from premises for unauthorized, personal, or unknown reasons
- Copying company or classified information unnecessarily
- Engaging in classified conversations without a need-to-know
- Establishing unauthorized means of access to company or customer information systems
- Seeking access to company proprietary, controlled sensitive, or classified information on subjects not related to job duties

Other behaviors that might indicate a possible insider threat include:

- Unreported foreign contacts or overseas travel
- Sudden reversal of financial situation or repayment of large debts or loans

If you observe any of these behaviors or suspicious behaviors by an individual, report the activity to your management, Security, or the Security Reporting website.
While not all suspicious behaviors or circumstances represent a threat, each situation must be examined along with information from other sources to determine whether or not there is a risk. Observing even a single activity and not reporting it can increase the potential damage that can be done.

Case Example: Go with your Gut

Ana Belen Montes was recruited by Cuba after learning of her views against the U.S. policies towards Central America. At that time she was a clerical worker in the Dept. of Justice. She went to work for the Defense Intelligence Agency and became the DIA’s top Cuban analyst.

While security officials became aware of her disagreement with U.S. foreign policy and had concerns about her access to sensitive information, she had passed a polygraph test.

According to a FBI news story, in 1996 “an astute DIA colleague – acting on a gut feeling – reported to a security official that he felt Montes might be under the influence of Cuban intelligence.” She was interviewed, but admitted nothing.

Four years later when the FBI was working to uncover an unidentified Cuban agent, the security official recalled the interview and contacted the FBI. An investigation was opened that led to her arrest and conviction.

References:
- CTM J303 – Insider Threat Program
- Find Security contact information on your sector home webpage or on the Employee Services website select Security & Access.
- Find other resources in the Counterintelligence & Insider Threat section on the Enterprise Security webpage

THREAT LANDSCAPE

The U.S. cleared industry is a prime target of many foreign intelligence collectors and government economic competitors attempting to gain military and economic advantages.

Cyberspace enables social engineering attacks with readily available information about businesses and people.

For example, spear phishing attacks use social engineering to trick an individual into providing information or clicking on a link or attachment containing malicious software that can provide unauthorized network access, ex-filtrate information, or do other harm.

Report spear phishing and suspicious activity, for example anomalous computer behavior to the CSOC at CSOC@ngc.com or 1- 877-615-3535.
ADVERSARY METHOD: ELICITATION

Elicitation is the strategic use of conversation to subtly extract information about you, your work, or your colleagues. Foreign intelligence officers are trained in elicitation tactics.

The Internet and social networking sites make it easier to obtain information to create plausible cover stories. Unsuspectingly, a conversation or relationship that starts out purely social gradually provides information or part of a puzzle that the foreign operative can combine with other information.

Employees should always be aware of the possibility of elicitation attempts both at work and in casual settings. Be prepared by knowing what information you cannot share and be suspicious of those who seek that information. If you believe someone is attempting to elicit information, you can say you don’t know, refer them to the Internet, try and change the topic, or provide a vague answer.

Because elicitation is subtle and can be difficult to recognize, report any suspicious conversations to Security or the Security Reporting website.

Attending a trade show or conference? Understand the limits of information you can provide. Report contacts if you experience insistent questions outside of the scope of what you have already provided, or attempts at unnecessary ongoing contact.

Are you a subject matter expert? Report unsolicited requests for assistance; requests to review thesis papers, drafts publications, or research-related documents; or unsolicited invitations to attend international conferences.

Don’t reply to unsolicited requests for information. Suspicious email can be reported to the Cyber Security Operations Center at CSOC@ngc.com. Report suspicious phone contacts to the Security Reporting Website.

Safeguards When Participating in External Conferences

If you are participating at a conference or meeting as a speaker, discussion panelist, or moderator where you are identified as a Northrop Grumman employee, follow Corporate Policy CPA6 Employee and External Communications, or your sector's Communication procedure for clearance of public speeches.

- Don’t connect your laptop to conference-provided networks or connect to the company network using their computer kiosks.
- Beware of potential eavesdropping when having work-related conversations in-person or over the phone.
- Report unusual contact attempts or occurrences to Security.

Reference:
- Where to Report webpage
• Security Points of Contact [webpage](#)

---

**ADVERSARY METHOD: RECRUITMENT**

Recruitment is obtaining cooperation from someone to provide information.

Anyone with information or access to information could be a potential target. Safeguard your actions and words to avoid becoming an easy target.

**You may not realize at first that you have been spotted for possible recruitment. In initial contacts the adversary will try to determine if you have information or access of value, or if you might have such information in the future.**

If the adversary is interested, he or she will attempt to develop the relationship and devise a ruse to establish a logical basis for continuing contact. The adversary will continue to assess your willingness to provide information.

The adversary’s goal is to establish a relationship of friendship and trust. It could start with requests such as professional advice or information about a co-worker. You might have a sense of obligation and not see any harm in complying. The adversary could then move the relationship along and step-up the information requests, for example, as a consultant.

Use caution if you feel you are being recruited.

- Listen carefully
- Be observant
- Remember as many details as possible
- Keep all options open by neither agreeing or refusing to cooperate
- Stay calm
- Be non-committal
- Ask for more time

Inform your security officer immediately if you have any suspicious conversations or suspect you are being recruited.

You are not being asked to avoid all foreign contacts. Your main defense against espionage is being aware of the signs of recruitment and elicitation, knowing not to respond to even seemingly casual questions for more information about the work that you do, and reporting all suspicious contacts to your Security office. Contacts can come in various forms, either in-person or online.
Case Example: As Much Time as it Takes

In 2010, ten deep-cover Russian spies were arrested. The individuals in the group married, bought homes, and had children as they appeared to assimilate into American life while actively collecting information and spotting and assessing potential recruits.

Reference:
- Where to Report webpage
- Security Points of Contact webpage

REPORTING

Compliance with security requirements is an on-going part of your position. The purpose of reporting possible threats and compromises is to detect and mitigate any vulnerability to our country and its resources, which includes Northrop Grumman and our employees.

Immediate threats and security compromises should be reported directly to your local Security team. The Security Reporting Website can be used to report suspicious activity, including insider threat, and suspicious contacts. These reports will be sent to your site specific designee.

Northrop Grumman employees are encouraged to report within company channels prior to contacting the government defense hotline. However, if you are not satisfied with the results of your contact at the company level, you are encouraged to report to the DoD hotline. Comments and questions made during these contacts must be kept unclassified.

- Phone: 800-424-9098
- Government e-mail: hotline@dodig.osd.mil
- Web: http://www.dodig.mil/hotline

If your report deals with a special access program please use that approved reporting method versus the process described here.

Reference:
- CSOC (Cyber Security Operations Center): CSOC@ngc.com or 1-877-615-3535 monitored 24x7
- Ethics and Business Conduct website for links to Business Conduct Officers and OpenLine
CONTACT INFORMATION

This concludes your annual Insider Threat Awareness training.

For questions or guidance contact your local security representative, or call the Enterprise Security Shared Service at 855-737-8364; option 3, option 2.

If you are NOT viewing this course in Learning Exchange (LX), email the ESSS Training Group at ESSS_DoDTraining@ngc.com stating you have completed the Insider Threat Awareness training and include:

- Your legal first and last name
- Your MyID
- The training confirmation code (ITT17)