Student Guide: Insider Threat Awareness

Introduction

Opening

Witness testimony: I always thought that guy acted a little strange. He complained a lot. His schedule was odd. He came in at odd hours. And he asked a lot of questions, maybe too many questions.

Would you recognize a threat from the inside?

Witness testimony: But there wasn't really that one thing and it wasn't my place to say anything. It's like an unwritten rule. We're a team. You don't report on your co-workers.

What would you do?

Witness testimony: I never thought anything like this could happen here.

If you see something, say something.

The Insider Threat

Who could become an insider threat? You've probably heard of the notorious cases: those who took secrets and those who took lives; those who risked their organizations and those who risked national security. But there are also unwitting insiders—people with access to information who unknowingly reveal more than they should.

An insider threat is anyone with authorized access to the information or things an organization values most, and who uses that access - either wittingly or unwittingly - to inflict harm to the organization or national security. When an insider becomes a threat, it can have far-reaching consequences on organizations, companies, and national security.

As a cleared employee working for the DoD, a Federal agency, or in cleared industry, you play an important role in protecting against insider threats.

What Does an Insider Look Like?

Witness testimony: I was looking for a bad guy. I never thought it could be my friend. I never thought he'd hurt our organization.

What do insider threats look like? They look like you and me. They look like your friends and neighbors. They can be anyone and they can target anything. Sometimes they are unwitting and simply create vulnerabilities for others to exploit. In addition to classified information, proprietary information, trade secrets, intellectual property, and the security of personnel may be threatened.

Malicious insiders go after anything they can use to inflict harm. They have many motivations: Some do it for money, while others do it for ego. Others do it for a cause or another country. Others do it simply because they can.

There are many cases of insiders betraying the trust of their organizations and their country, including those listed here.

Workplace Violence

James Wells was a civilian employee at the Coast Guard Communications Station Kodiak in Alaska. On April 12, 2012, Wells entered the communications rigger shop where he shot and killed two co-workers with a .44-caliber revolver.

Wells had a work record of habitual poor performance. He had been cited several times for being absent from the work area and was told in December 2011 by his supervisor to "be a part of the process or retire." A month later, the supervisor informed Wells that others would attend an annual conference in his stead due to his disciplinary problems. A heated discussion followed.

Subsequent FBI investigation indicated that Wells had shown numerous indicators of a potential insider threat. He was known to be a disgruntled, substandard civilian employee who frequently feuded with co-workers and supervisors. Wells failed to follow regulations and guidelines and had displayed a temper and falsely accused co-workers of theft. His work record included numerous reprimands, disciplinary sanctions, and theft of government fuel.

Wells was initially convicted of murder. An appeals court vacated the decision on technical grounds. Neither Wells guilt nor the investigation were the basis for the ruling. The decision is pending further appeal.

Economic Espionage

Walter Liew was a naturalized American citizen, business owner, and research engineer who stole DuPont Corporation's protocols for producing its superior titanium white and sold them to the Panang Group companies in China for more than $20 million. Liew even took blueprints for a factory and used the information to win contracts worth almost $30 million.

Liew was convicted of violations of the Economic Espionage Act, tax evasion, bankruptcy fraud, and obstruction of justice on March 6, 2014. His conviction was the first federal jury conviction under the Economic Espionage Act. He was sentenced to 15 years in prison, forfeiture of $27.8 million, and $511,000 in restitution to DuPont.

Prior to his arrest, Liew showed numerous potential espionage indicators. First, he traveled extensively throughout China to market his stolen information. Liew also owned

multiple foreign companies and made numerous foreign contacts. In addition, Liew demonstrated unexplained affluence, owning an expensive Mercedes SUV and a luxury condominium in Singapore. Finally, Liew had sought access to areas of information where he did not have a "need-to-know."

As a result of Liew's economic espionage, DuPont lost valuable research that impacted numerous projects. Long-held trade secrets were disclosed to competitors and the public, and profits from current and future projects were compromised.

Unauthorized Disclosure

Benjamin Bishop, a government contractor and retired U.S. Army Lieutenant Colonel, damaged national security through the unauthorized disclosure of Secret classified information. Unauthorized disclosure occurs when an employee causes the unsanctioned release of information. Examples include media leaks and the posting of sensitive information online. Note that whistleblowing via proper channels is not an unauthorized disclosure.

Specifically, Bishop emailed classified information to a Chinese woman who he met at an international defense conference, formed a romantic relationship with, and was in the United States as a graduate student on a J-1 visa. In the email, he provided Secret information related to joint training and planning sessions between the United States and the Republic of Korea as well as a classified photograph of a Chinese naval asset.

Despite his unblemished security record, Bishop became prey to an effective recruitment technique. His insider threat indicators included undisclosed foreign contact, personal conduct (he was having an affair with the foreign contact), bringing classified material home, and unreported foreign travel.

He pled guilty on March 13, 2014 for unlawfully retaining classified national defense information at his home and for willfully communicating classified national defense information to a person not authorized to receive it. Bishop was sentenced to 87 months in prison and 3 years of supervised release.

Indicators of a Potential Insider Threat

See What?

Witness testimony: I always thought that guy acted a little strange. But there wasn't really that one thing.

If faced with a threat from an insider, would you recognize it?

In your day-to-day interactions with your coworkers, you notice the following. Which, if any, may be an indicator of an insider threat?

Select all that apply. Then check your answers on the next page.

- ☐ While helping a coworker with a new system, you notice her computer contains Confidential files related to a project she is not working on and has no need-to-know.
- ☐ On your way to a meeting, you overhear two coworkers discussing classified information in an office corridor.
- ☐ During a meeting, a coworker shows off an expensive new watch. When asked about affording such a luxury, he becomes uncomfortable and offers no explanation.
- ☐ As you arrive at your building early one morning, you encounter a coworker leaving the building. The coworker nervously explains that he sometimes prefers to work overnight without the distraction of others.

Major Categories

All of these things might point towards a possible insider threat. Examining past cases reveals that insider threats commonly engage in certain behaviors. For example, not all insiders act alone.

While some insiders volunteer, others are targeted and recruited by adversary groups. For this reason, you should be aware of common signs someone is being recruited. And once an insider turns on his or her organization, that person will start collecting information. So you need to be able to detect clues that that might be happening. Once they have information, insiders must then transmit it. If you know the signs of information transmittal, you will be better prepared to detect it. And insiders often exhibit other common suspicious behaviors you need to know about.

Not all of these indicators will be evident in every insider threat and not everyone who exhibits these behaviors is doing something wrong. However, most of the insider threats we have discovered displayed at least some of these indicators. It is important for you to be aware of these behaviors so you can combat the insider threat and protect your organization and the country.

Recruitment

Witness testimony: I did wonder how he kept up with his bills, but it wasn't my place to say anything.

While not all insiders are recruited, those who are are often recruited slowly over time. Classic recruitment by adversaries includes three phases: spot and assess, development, and recruiting and handling.

First, intelligence officers spot and assess individuals for potential recruitment. Adversaries are not necessarily looking to target someone with a high level of access. Sometimes the potential for future access or the ability of the recruit to lead to other high value targets is enough to generate adversary interest. Spot and assess can take place anywhere, but is always approached in a non-threating and seemingly natural manner. Put yourself in the place of an intelligence officer. How would you recruit a computer scientist? Perhaps at a trade show or through a business contact or perhaps at a computer store or at a social event. Even online venues, such as chat rooms and social media, are used for this process. During the spot and assess phase, the foreign intelligence agent often explores potential exploitable weaknesses that may be used as a lever against the recruit. These could include drugs or alcohol, gambling, adultery, financial problems, or other weaknesses.

Once a potential recruit has been identified, adversaries begin to cultivate a relationship with that individual. In the development phase, meetings with the recruit will become more private and less likely to be observable.

By the time the recruitment and handling phase is initiated, the individual is likely emotionally tied to the adversary. The actual recruitment may involve appeals to ideological leanings, financial gain, blackmail or coercion, or any other of a number of motivators unique to that recruit. Recruitment almost always involves contacts with individuals or organizations from foreign countries. However, an already committed U.S. spy may attempt to recruit colleagues.

Indicators of recruitment include signs of sudden or unexplained wealth and unreported foreign travel.

Recruitment Indicators

Reportable indicators of recruitment include, but are not limited to:

- Unreported request for critical assets outside official channels
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Contact with an individual who is known to be, or is suspected of being, associated with foreign intelligence, security, or terrorism
- Unreported offer of financial assistance, gifts, or favors by a foreign national or stranger: Beware of those bearing gifts
- Suspected recruitment by foreign or domestic competitive companies to convince employee to work for another company

Critical Assets

Assets essential to an organization's mission or to national security that, if exploited, could result in serious harm; include:

- Classified information
- Proprietary information
- Intellectual property
- Trade secrets
- Personnel security
- Other information that could compromise or harm your organization's resources, including information, facilities, or personnel

Information Collection

Witness testimony: He asked a lot of questions….maybe too many questions.

Before someone can steal information, they must first collect the information. It can be intentionally stolen by a malicious insider or a person may have it already – and then inadvertently leak it. Insiders may physically remove files, they may steal or leak information electronically, or they may use elicitation as a technique to subtly extract information about you, your work, and your colleagues. When done well, elicitation can seem like simple small talk.

Regardless of the method used, anytime a person attempts to access or record information without authorization, regardless of intent, it should be of concern.

Information Collection Indicators

Reportable indicators of information collection include, but are not limited to:

- Unauthorized downloads or copying of files, especially for employees who have given notice of termination of employment
- Keeping critical assets at home or any other unauthorized place
- Acquiring access to automated information systems without authorization
- Operating unauthorized cameras, recording devices, computers, or modems in areas where critical assets are stored, discussed, or processed
- Asking you or anyone else to obtain critical assets to which the person does not have authorized access
- Seeking to obtain access to critical assets inconsistent with present duty requirements

Actions/behaviors specific to classified information:

- Asking for witness signatures certifying the destruction of classified information when the witness did not observe the destruction

Information Transmittal

Witness testimony: Looking back, there were signs. He'd talk about anything—even classified information—anywhere. He didn't care who was around.

Insiders must have a way to transmit the information they are compromising. If you notice someone showing signs of transmitting information without authorization or outside of approved channels, you should pay attention. Behaviors you might observe include removing assets or information without authorization, extensive use of systems or equipment, and discussing information in unauthorized areas or by unauthorized means.

If you notice someone failing to follow procedures for safeguarding, handling, and transmitting classified information, it may be a sign of an insider threat.

Information Transmittal Indicators

Reportable indicators of information transmittal include, but are not limited to:

- Removing critical assets from the work area without appropriate authorization
- Extensive use of copy or computer equipment to reproduce or transmit critical asset-related information that may exceed job requirements
- Discussing critical asset-related information in public or on a non-secure telephone

Actions/behaviors specific to classified information:

- Using an unauthorized device or computer to transmit classified information
- Attempting to conceal any foreign travel
- Improperly removing the classification markings from documents

General Suspicious Behavior

Witness testimony: I always thought that guy acted a little strange. His schedule was odd. He'd come in after hours when no one else was around.

Once an insider threat is revealed, coworkers often recall signs that something wasn't right. An insider threat may exhibit a number of suspicious behaviors, including working outside of regular duty hours, repeatedly failing to follow processes and policies which result in security violations, or displaying signs of unexplained affluence.

Please note that none of these indicators alone mean that an individual poses an insider threat. In fact, many indicators are often easily explained or represent a personal issue that poses no threat to the organization.

General Suspicious Behavior

Reportable indicators of other suspicious behaviors include, but are not limited to:

- Attempts to expand access:
  - Attempting to expand access to critical assets by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities
  - Performing repeated or unrequired work outside of normal duty hours, especially unaccompanied
- Questionable behavior:
  - Exhibiting behavior that results in repeated security violations
  - Engaging in illegal activity or asking you to engage in any illegal activity
- Changes in financial circumstances:
  - Displaying unexplained or undue affluence explained by inheritance, luck in gambling, or some successful business venture
  - Displaying sudden reversal of financial situation or sudden repayment of large debts
- Attempts to compromise individuals:
  - Attempting to entice personnel with access to critical assets into situations that could place them in a compromising position
  - Attempting to place personnel with access to critical assets under obligation through special treatment, favors, gifts, money, or other means
- Questionable national loyalty:
  - Displaying questionable loyalty to U.S. government or company
  - Making anti-U.S. comments

- Exhibits actions or behaviors associated with disgruntled employees:
  - Conflicts with supervisors and coworkers
  - Decline in work performance
  - Excessive tardiness
  - Unexplained absenteeism
- Failure to report information as required under federal investigative standards, such as:
  - Foreign travel
  - Foreign contacts
  - Security violations
  - Criminal conduct
  - Drug or alcohol abuse
  - Other personal behaviors and activities

Reporting

Say What?

Witness testimony: We all went to the training. We sat through the briefings. Yet, when we actually saw signs something wasn't right, we did nothing. Why didn't someone say something?

If faced with a threat from an insider, would you know what to do? Would you know how to report it?

You notice a coworker is demonstrating some of the behaviors of an insider threat. Do you know the channels you should use to report it?

Select your response. Then check your answer on the next page.

- ○ Yes; I know exactly what to do and would report it immediately.
- ○ I'm not sure; I'd have to look it up or check with somebody.
- ○ No; I have no idea what I should do… maybe call the hotline?

Reporting Procedures

Witness testimony: I did feel like something wasn't right. And I did think I should say something. I just didn't know who to go to.

If you suspect a possible insider threat or possible recruitment attempts, you must report it. You cannot assume someone else will do so. Every one of us is an owner of security - both the security of information and the security of resources including personnel, facilities, and information systems. We are all responsible for their safekeeping.

A major hurdle that deters people from reporting is the idea that they are snitching on a colleague. But your organization's Insider Threat Program is designed to identify and mitigate these issues by helping employees to resolve personal or workplace problems before they escalate into threatening behaviors or result in recruitment attempts by our adversaries. When you report issues, the Program draws upon resources from security, mental health professionals, counterintelligence, law enforcement, human resources, and more to get people the help they need and to safeguard your security, the security of your fellow colleagues, and the resources and capabilities of your organization.

Insider threat reporting procedures vary depending on whether you are an employee of the DoD, a Federal agency, or you work in cleared industry.

Reporting Requirements for DoD

DoD employees must report potential threats to their organization's Insider Threat Program. You may also consult your security office or supervisor. Insider Threat Program personnel will coordinate with counterintelligence elements and law enforcement, if required. Remember, you may have additional reporting requirements under counterintelligence and security policies that must be followed regardless of whether an insider is involved.

Federal Agency Reporting Procedures

If you are an employee of a Federal agency, report to your agency's Insider Threat Program or security office or to your supervisor. Follow your agency-specific reporting procedures.

Reporting Requirements for Cleared Industry

Employees of cleared industry must report potential threats to the facility Insider Threat Program Senior Official (ITPSO) or Facility Security Officer (FSO). Depending on the situation, the FSO will then report the possible threat to the facility's ITPSO, DSS Industrial Security Representative, DSS Counterintelligence Specialist, and, if it involves known or suspected espionage, to the FBI. Remember, you are still required to report suspicious contacts and other reportable behaviors in accordance with the National Industrial Security Program Operating Manual (NISPOM).

Failure to Report

Witness testimony: I never thought anything like this could happen. Why didn't someone say something?

Unfortunately, insider threats often go unreported until it is too late. In the majority of past cases, relevant information was available, yet went unreported. How different might things have been had someone said something?

When you fail to report, you risk both your physical security and the information security of your organization. Insider threats weaken the U.S. military's battlefield advantage and jeopardize war fighters. They increase our vulnerability to fraud, terrorist activity, and cyber-attacks. If you are a member of cleared industry, an insider may cost your company its business and you your job.

Failing to report also fails the employee who needs help. When you don't report, you lose the opportunity to help your coworker resolve problems before becoming an insider threat.

DoD and Federal employees may be subject to both civil and criminal penalties for failure to report. For cleared defense contractors, failing to report may result in loss of employment and security clearance. Individuals may also be subject to criminal charges.

You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense.

Conclusion

You have just learned how insider threats affect the DoD, Federal agencies, cleared industry, and people like you. You need to be aware of these threats. You need to consider your facility, its technology and programs, and the information you know. How might you be targeted? If you suspect a potential insider threat, you must report it.

To receive course credit, you must take the Insider Threat Awareness examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.