FACT SHEET
U.S. Army Cyber Command

The Nation's Army in Cyberspace

www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

THE FACTS: INSIDER THREATS

Organizations can often mitigate the threat of outsiders stealing their property, either physically or electronically. But the insider -- the employee with legitimate access – can be much harder to detect and stop. Whether stealing for personal gain or conducting espionage, someone who steals information or products to benefit another organization or country can do serious damage. Foreign governments intent on illegally acquiring information may try to recruit existing employees to do the job for them.

What motives or personal situations increase the likelihood someone will spy on their agency?

- Greed or financial need such as excessive debt or overwhelming expenses.
- Anger, revenge or disgruntlement to the point of wanting to retaliate against the organization.
- Problems at work such as lack of recognition, disagreements with coworkers or managers, dissatisfaction with the job, or a pending layoff.
- Ideology or identification: A desire to help the "underdog" or a particular cause.
- Divided loyalty: Allegiance to a country other than the United States.
- Adventure or thrill: "James Bond wannabes" who wanting to add excitement to their lives.
- Drug or alcohol abuse, family and conflict, extramarital affairs, gambling, fraud or other illicit behavior can give foreign governments leverage to blackmail people into spying.
- Large egos and people who believe they are "above the rules" or are looking to repair wounds to their self-esteem may be vulnerable. Flattery or the promise of a better job could entice them to spy for a foreign agency.
- A desire to please or win the approval of someone who could benefit from insider information can motivate a potential spy.

What organizational situations can increase the likelihood of information theft?

- Providing access privileges to those who do not need them.
- The availability and ease of acquiring proprietary, classified, or other protected materials.
- Proprietary or classified information that is not labeled or is incorrectly labeled.
- The ease that someone may exit the facility (or its networks) with proprietary, classified or other protected materials.
- Undefined policies regarding working from home on projects of a sensitive or proprietary nature.
- The perception that security is lax and the consequences for theft are minimal or non-existent.
- Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials.
- Employees who are not trained on how to protect proprietary information.

ABOUT US: **United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.**

What behaviors may indicate that an employee may be spying and/or stealing information?

- Taking proprietary or other material home (documents, thumb drives, computer disks, or e-mails) without the need or authorization.
- Inappropriately seeking or obtaining proprietary or classified information on subjects not related to their work duties.
- Showing interest in matters outside the scope of their duties, particularly those of interest to foreign entities.
- Unnecessarily copying material, especially if it is proprietary or classified.
- Remotely accessing the computer network while on vacation, sick leave, or at other odd times.
- Disregarding company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches or downloading confidential information.
- Working odd hours without authorization or showing notable enthusiasm for overtime work, weekend work or unusual schedules when clandestine activities could be conducted more easily.
- Not reporting overseas travel or foreign contacts (particularly contact with foreign government or intelligence officials).
- Taking repeated short trips to foreign countries for unexplained or seemingly unusual reasons.
- Unexplained affluence -- buying things they could not normally afford on their income.
- Engaging in contact with suspicious individuals.
- Showing unusual interest in the personal lives of coworkers and asking inappropriate questions regarding finances or relationships.
- Expressing concern that they are being watched or investigated.

What can organizations do to deter spying and theft?

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is well protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure that security (including computer network security) personnel have the tools they need.
- Remind employees that reporting security concerns is vital to protecting the organization, its reputation, its well-being and its future.

Source: https://www.fbi.gov/about-us/investigate/counterintelligence/history-and-evolution

Follow ARCYBER on
(click the images to visit our pages)

ABOUT US: **United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.**

As of 2 March 2016