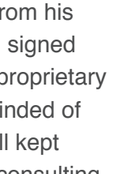
RECENT INSIDER THEFT CASES

Michael Mitchell, a sales clerk and engineer, became disgruntled and was fired from his job based on poor performance. Mitchell signed statements affirming he had returned all proprietary information to his employer and was reminded of nondisclosure policies. However, Mitchell kept numerous computer files, entered into a consulting agreement with a rival Korean company, and provided trade secrets from his former employer to that company. In March 2010, he was sentenced to 18 months in prison and ordered to pay his previous employer over $187,000.

Shalin Jhaveri, a technical operations associate, gave trade secrets to a person he believed was an investor willing to finance a business venture in India, and confirmed to the investor that the information he had taken from his employer was everything he needed to start the business. He confessed that he disguised his actions to evade detection. In January 2011, he was sentenced to time served (one year and fifteen days), three years probation, a $5,000 fine, and a $100 Special Assessment.



David Yen Lee accepted a job on 27 February 2009 from a business competitor in China, but did not resign from his current employer until 16 March 2009. Lee admitted to downloading trade secrets from his employer's secured computer system for several months prior to his resignation. The stolen trade secrets were worth between $7 million and $20 million. In December 2010, Lee was sentenced to 15 months in prison and three years supervised release.

Sergey Aleynikov, a computer programmer, worked for a company on Wall Street from May 2007 until June 2009. During his last few days at that company, he downloaded, and transferred 32 megabytes of proprietary computer codes– a theft that could have cost his employer millions of dollars. He hoped to use the computer codes at his new Chicago-based employer. He attempted to hide his activities, but the company discovered irregularities through its routine network monitoring systems. In December 2010, Aleynikov was found guilty of theft of trade secrets and transportation of stolen property in foreign commerce.

Greg Chung spied for China from 1979-2006. Federal charges against Chung consisted of stealing trade secrets about the space shuttle, the Delta IV rocket and the C-17 military cargo jet for the benefit of the Chinese government. Chung's motive was to "contribute to the Motherland." He was an engineer that stole hundreds of thousands of documents. He traveled to China under the guise of giving lectures while secretly meeting with Chinese government officials and agents. He was also encouraged to use Chi Mak (see below) to transfer information back to China. Chung was arrested in February 2008 and in February 2010 he was sentenced to over 15 years in prison.

Chi Mak admitted that he was sent to the United States in 1978 in order to obtain employment in the defense industry with the goal of stealing US defense secrets, which he did for 20 plus years. He most recently passed information on quiet electric propulsion systems for the next generation of US submarines, details on the Aegis radar system, and information on stealth ships being developed by the US Navy. The Chinese government tasked Mak to acquire information on other specific technologies. Mak recruited family members to encrypt and covertly courier information back to China. In May 2007, Chi Mak was convicted of conspiracy, attempting to violate export control laws, failing to register as an agent of a foreign government, and making false statements to investigators. He was sentenced to over 24 years in prison, and four members of his family received varying sentences of up to 10 years in prison.

For additional information, training, or assistance, contact the FBI.
www.fbi.gov

U.S. Department of Justice
Federal Bureau of Investigation

A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically, and can mitigate the threat of an outsider stealing company property. However, the thief who is harder to detect and who could cause the most damage is the insider–the employee with legitimate access. That insider may steal solely for personal gain, or that insider may be a "spy"–someone who is stealing company information or products in order to *benefit another organization or country.*

THE INSIDER THREAT

An introduction to detecting and deterring an insider spy

- Disgruntled
- Working odd hours
- Unexplained affluence
- Unreported foreign travel

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company's trade secrets.

PROTECT YOUR INTELLECTUAL PROPERTY

Theft of intellectual property is an increasing threat to organizations, and can go unnoticed for months or even years.

There are increased incidents of employees taking proprietary information when they believe they will be, or are, searching for a new job.

Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business.

A domestic or foreign business competitor or foreign government intent on illegally acquiring a company's proprietary information and trade secrets may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing.

PERSONAL FACTORS

There are a variety of motives or personal situations that may increase the likelihood someone will spy against their employer:

Greed or Financial Need: A belief that money can fix anything. Excessive debt or overwhelming expenses.

Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization.

Problems at work: A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.

Ideology/Identification: A desire to help the "underdog" or a particular cause.

Divided Loyalty: Allegiance to another person or company, or to a country besides the United States.

Adventure/Thrill: Want to add excitement to their life, intrigued by the clandestine activity, "James Bond Wannabe."

Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Ego/Self-image: An "above the rules" attitude, or desire to repair wounds to their self-esteem. Vulnerability to flattery or the promise of a better job. Often coupled with Anger/Revenge or Adventure/ Thrill.

Ingratiation: A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.

Compulsive and destructive behavior: Drug or alcohol abuse, or other addictive behaviors.

Family problems: Marital conflicts or separation from loved ones.

ORGANIZATIONAL FACTORS

Organizational situations may increase the ease for thievery:

The availability and ease of acquiring proprietary, classified, or other protected materials. Providing access privileges to those who do not need it.

Proprietary or classified information is not labeled as such, or is incorrectly labeled.

The ease that someone may exit the facility (or network system) 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, or not fully consider the consequences of their actions.

Employees are not trained on how to properly protect proprietary information.

BEHAVIORAL INDICATORS

Some behaviors may be a clue that an employee is spying and/ or methodically stealing from the organization:

Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail.

Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.

Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.

Unnecessarily copies material, especially if it is proprietary or classified.

Remotely accesses the computer network while on vacation, sick leave, or at other odd times.

Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.

Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.

Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.

Short trips to foreign countries for unexplained or strange reasons.

Unexplained affluence; buys things that they cannot afford on their household income.

Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

Overwhelmed by life crises or career disappointments.

Shows unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships.

Concern that they are being investigated; leaves traps to detect searches of their work area or home; searches for listening devices or cameras.

Many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime.

YOU CAN MAKE A DIFFERENCE

Organizations need to do their part to deter intellectual property theft:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, 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 security (to include computer network security) personnel have the tools they need.

Remind employees that reporting security concerns is vital to protecting your company's intellectual property, its reputation, its financial well-being, and its future. They are protecting their own jobs. Remind them that if they see something, to say something.

GET ASSISTANCE

Being aware of potential issues, exercising good judgment, and conducting discrete inquiries will help you ascertain if there is a spy in your midst. However, if you believe one of your employees is a spy or is stealing company trade secrets, do not alert the person to the fact that he/she is under suspicion, but seek assistance from trained counterintelligence experts–such as the FBI. The FBI has the tools and experience to identify and mitigate such threats. If asked to investigate, the FBI will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality. The FBI is committed to maintaining the confidentiality and competitive position of US companies. The FBI will also provide security and counterintelligence training or awareness seminars for you and your employees upon request.