Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations

June 2009

Derrick Spooner
Dawn M. Cappelli
Andrew P. Moore
Randall F. Trzeciak

This work was funded by

\

Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations

This report is the third in the quarterly series, *Spotlight On*, published by the Insider Threat Center at CERT and funded by CyLab. Each report focuses on a specific area of concern and presents analysis based on hundreds of actual insider threat cases cataloged in the CERT insider threat database. For more information about CERT's insider threat work, see http://www.cert.org/insider_threat/.

In this article, we focus on current or former employees, contractors, or business partners who stole intellectual property (IP), such as source code, scientific formulas, engineering drawings, strategic plans, or proposals from their organizations to benefit a foreign entity. We drew the case material from a mixture of court documents, Department of Justice press releases, and media reports. As in the previous articles in this series, we begin by explaining the criteria used to select cases for this article. Next, we provide a snapshot that focuses on the questions of who, what, where, when, why, and how. Then, we provide a summary of the relevant details of those cases. Finally, we provide a series of recommendations that could potentially mitigate the risk of similar occurrences.

Snapshot of the Insiders

The cases included in this article fit the problem described in the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07* prepared by the Office of the National Counterintelligence Executive:

> *The United States remains the prime target for foreign economic collection and industrial espionage as a result of its worldwide technological and business leadership Indeed, strong US international competitiveness underlies the continuing drive by foreign collectors to target US information and technology.*[1]

In all of the cases presented here, malicious insiders misused a company's systems, data, or network to steal intellectual property from an organization inside the U.S. for the benefit of a foreign entity – either an existing foreign organization or a new company that the insiders established in a foreign country. The cases also exhibit activities defined by the Office of the National Counterintelligence Executive as economic espionage or industrial espionage:

> ***Economic Espionage*** *- which is the conscious and willful misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent.*[2]
>
> ***Industrial Espionage*** *- which is the conscious and willful misappropriation of trade secrets related to, or included in, a product that is produced for, or placed in, interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret.*[3]

[1] See http://www.ncix.gov/publications/reports/fecie_all/fecie_2007/FECIE_2007.pdf
[2] See http://www.ncix.gov/publications/reports/fecie_all/fecie_2007/FECIE_2007.pdf
[3] See http://www.ncix.gov/publications/reports/fecie_all/fecie_2007/FECIE_2007.pdf

This article does not include the theft or modification of other confidential information such as personally identifiable information (PII) or credit card information. Our insider threat research has determined that the "profile" of those types of crimes differs from that observed in theft of IP crimes, so we will focus only on theft of intellectual property. CERT published a report describing the profile of insider theft of intellectual property in June 2009.[4]

Cases that involve foreign beneficiaries can differ from other theft of IP cases because the insiders may have a sense of duty or loyalty to their countries of origin that overrides any loyalty to their employer. Moreover, some of these cases suggest that some foreign entities appear to be interested in recruiting insiders to steal IP to advance businesses in that particular country. Competing loyalties, coupled with recruitment of employees in U.S. businesses by foreign nations or organizations, make this type of crime a potent threat for organizations that rely on IP for competitive advantage.

There are several reasons for heightened concern about this kind of crime. The impact of a crime that extends outside the jurisdiction of U.S. law enforcement on an organization can be substantially greater than a case that remains within U.S. jurisdiction. Insiders who leave the U.S may be difficult or impossible to locate and arrest. And even if the insider were located and arrested, extradition to the U.S. would be required. Therefore, there can be more risk from an employee who intends to leave the U.S. following the theft than from employees contemplating criminal acts against their employer who intend to remain in the U.S.

In addition, it can be very difficult to recover stolen IP once it leaves the U.S. In cases within U.S. borders, the company that receives the stolen IP can suffer similar consequences under the same laws as the insiders if they use the stolen IP for their own advantage. Thus, domestic organizations are under greater obligation to cooperate with authorities and return all stolen IP than foreign organizations might be.

Who they are

Out of over three hundred cases cataloged in CERT's insider threat database, only ten involved individuals who stole to benefit a foreign entity. In these ten cases, all of the individuals worked as either a scientist or a computer engineer. Males committed nine of the ten incidents. Of the nine cases that identify citizenship, five insiders were naturalized U.S. citizens, and four were foreign nationals. Of those nine individuals, seven were Chinese and two were Taiwanese. One of the Chinese individuals was a naturalized Canadian citizen. Five of the cases involved at least one accomplice who was also an insider, and at least two of those accomplices shared the same country of origin as the primary insider.

What they stole

All of the insiders stole intellectual property in digital form, physical form, or both. Two of the cases included a potential financial loss that exceeded several hundred million dollars. Four insiders stole software, including proprietary source code. Six of the insiders exfiltrated sensitive product information, such as data sheets, design schematics, or formulas. Three cases involved the theft of information that was clearly outside the scope of the insiders' job duties, yet they appeared to be able to access the information without the need to

[4] Moore, A.P., D.M. Cappelli, T. Caron, E. Shaw, R.F. Trzeciak, "Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model," in Proc. Of the 1st International Workshop on Managing Insider Security Threats (MIST2009), Purdue University, West Lafayette, USA, June 16, 2009.

escalate their access privileges. The other seven cases did not specify whether they accessed information within or outside their "need to know."

Where and When they steal

Eight of the insiders stole the information while on site, and one insider stole both while on site and via a remote VPN connection. Six insiders stole the information during normal business hours, one well outside of normal working hours, and one both during and outside of normal working hours. In all of the cases, the insiders began their theft while still employed at the victim organizations. Only one case clearly identified that the insider continued to steal after she submitted a letter of resignation; however, the last theft occurred within a day of the resignation.

Why they steal

All of the insiders stole intellectual property for a business advantage. Their specific motives fall into two separate categories:

- **Theft of intellectual property to form a new competing business.** Four of the cases involved insiders stealing IP to establish a new business venture in a foreign country that would compete with the victim organization. In all four of these cases, the insiders had at least one accomplice (who was also an insider) who assisted them with their theft, with forming the new business, or with both.
- **Theft of intellectual property to take to a new employer in a competing business.** The remaining six cases involved insiders stealing IP to take it to their new employers, businesses located outside the U.S that competed with the victim organizations. In all six of these cases, the insiders had already accepted jobs with the competitors before leaving the victim organization.

How they steal

None of the insiders was known to have used any malicious code or to have exploited any technical vulnerability to perpetrate their thefts, as all of them had some level of access to the information they stole. However, in at least one of the cases, the insider successfully accessed information that did not pertain to his or her job duties without circumventing any known security mechanism or exceeding any explicit authorization level.

The insiders used methods such as

- Accessing the company's internal servers, either on site or using VPN and copying the information to their machines or to external media. One insider downloaded tens of thousands of proprietary files related to product technologies and development from a company's internal database.
- Physically stealing proprietary documents or hardware components, both during and after normal business hours. In one case, surveillance recorded the insider carrying large bags, multiple books, and a binder from the office the evening before resigning. Another insider stole over twenty boxes of physical research material from a supposedly "secure" environment.
- E-mailing information out of the organization using a personal email account on a company computer.

Summary of Cases

Summaries of the ten cases covered in this article follow. We have divided them into two groups:

- insiders who stole IP in order to form new competing businesses in collaboration with a foreign government or organization
- insiders who stole IP to take to their new employers in competing businesses outside the U.S.

Theft of intellectual property to form a new competing business in collaboration with a foreign government or organization

1. A senior engineer, his wife, and another accomplice who was a foreign national all worked for an auto parts manufacturer. The insider's wife quit her job as a vice president of sales, and conspired with the accomplice inside the organization to set up a new company. The trio intended to steal proprietary information from the auto parts manufacturer in the U.S, provide it to a foreign manufacturer, and then receive commissions on sales made by the foreign company. While still employed at the victim organization, the engineer was able to copy hundreds of files to CDs, including proprietary design and manufacturing process information. He then relayed this information to his wife, who proceeded to forward it to the external manufacturer. All three conspirators were convicted and sentenced to various amounts of jail time; however, the source material does not state whether the stolen IP was recovered.
2. Two engineers worked at a company that manufactured semiconductors. They conspired to steal proprietary design information from both the semiconductor company, and another company that had previously employed them. The two created a new company within the U.S. to develop and sell products based on the stolen intellectual property. They received venture capital for their new company from a foreign government. The authorities arrested the engineers and seized the stolen IP; however, they are still awaiting trial.
3. Two senior members of the technical staff at a telecommunications company worked on developing a sophisticated telecom device. While employed at the victim organization, they founded a new startup that supposedly served a similar but unique market niche. However, the two used this startup company to develop a prototype for a telecom device based almost entirely on the proprietary information they stole from their previous employer. These individuals met with a consultant hoping to obtain venture capital; however, when the consultant requested to see the prototype, they refused for fear of revealing their theft. Later, they met with a foreign business to request venture capital and propose a joint venture to market the stolen product with an existing company in the foreign country. The insiders physically stole hardware components and exfiltrated the proprietary information by email while still employed by the telecommunications firm. They then stored the information on their startup company's password-protected website in order to make it available to their foreign business partner. The individuals also made several trips to the foreign country to finalize the joint venture with the foreign company.

   The individuals used several methods to disguise their activity and remove their association with the startup company such as

   - using email addresses and a post office box that contained no record of their names
   - acquiring cell phones under their spouses' names
   - removing their names from the articles of incorporation of their startup company
   - removing their names from the Internet registry of their startup company's website

- using aliases (and obtaining business cards for these aliases) for all public communication regarding the startup company

Investigators uncovered a great deal of proprietary information in one insider's basement that included stolen hardware components of the telecom device. After being released on bail, the primary insider fled from authorities and remains at large. The status of the accomplice remains unknown, and the impact of divulging the IP to the foreign company was not specified.

4. The "lead" insider and an accomplice worked as engineers at two different victim organizations. In addition, the lead insider worked at two other victim organizations. From the four victim organizations, the individuals stole various IP and started a company funded by a foreign government to sell products based on the stolen information. The individuals attempted to recruit other insiders to steal information and work for their company. The resulting investigation revealed that both insiders possessed IP, including physical documents, in their homes. The accomplice had IP in his office at one of the victim organizations. Unfortunately, reports of the crime do not specify the exact timeframe of the insider's employment in the victim organizations or of the series of thefts. Both individuals were arrested and convicted, and authorities seized IP in the insiders' possession from all four victim organizations.

Theft of intellectual property to take to a new employer in a competing business outside the U.S.

1. The insider worked as a software engineer at a telecommunications company. While supposedly on medical leave from the victim company, she in fact worked for two other companies. For a short period, she worked for a local competitor whose equipment she used to access the victim organization's network and download proprietary documents. During the medical leave, she also began to work for a company in a foreign country. She returned from medical leave to the victim organization but had a one-way ticket to the foreign country scheduled to depart a few days later. During the interim between returning to work and fleeing the country, she downloaded hundreds of documents, including source code, from the victim's network. She also physically removed large amounts of proprietary material from the office. The insider was able to access documents that did not pertain to her work assignments at the victim organization. On her last day, the insider emailed her manager a letter of resignation while at work, then came back later in the evening to download even more technical documents. Before attempting to board the plane, Customs and Border Protection (CBP) officers randomly stopped the insider and asked how much currency she was carrying. The CBP officers uncovered much more cash than the amount she had declared and proceeded to inspect the rest of her carry-on luggage. They found documents marked as confidential and proprietary and confiscated them since the insider admitted that she did not actively work for the company whose name was on the documents. The victim organization estimated that releasing the IP would have cost them several hundred million dollars over three years. During the investigation, the victim organization identified the stolen materials and the insider was charged. The outcome of the trial is still pending. The source material did not state the extent to which any other IP was already transferred to the beneficiary organizations.

2. The insider worked as a chemist and later a product development director at a paint manufacturing plant. He made a business trip abroad to work with one of the victim organization's subsidiaries, and a coworker noticed that he was unusually interested in a foreign competitor. A few weeks after the trip, the insider resigned abruptly. This raised some suspicion at the victim organization. They investigated the company laptop he had returned and noticed that he had deleted all of the temporary files. Upon further examination, the organization discovered a hidden file that contained, among other things, a prohibited data copy program and 44 GB of unauthorized data that included IP. Upon executing a search warrant,

authorities confiscated a USB drive from the insider's luggage as he was attempting to leave the country. The drive contained IP belonging to the organization. The information included formulas for products that the insider had not worked on and thus had no legitimate reason to possess. The authorities also noticed that the insider's LinkedIn profile stated that he was now employed by a similar company in a foreign nation. The insider was arrested and charged, but trial has not adjourned.

3. The insider worked as a senior systems engineer at a visual simulation company. He was born in China, but held Canadian citizenship. He resigned from the victim organization and, at his exit interview, falsely stated that he returned all proprietary information as required by the IP agreement he had signed as precondition to employment. After he moved to a foreign country, the insider returned to the victim organization as an independent consultant and continued to access proprietary information. While serving as a consultant, he compiled and coerced others to compile proprietary source code in direct violation of company policy. Before terminating his consultancy with the victim organization, he accepted a job with a foreign competitor. After leaving the victim organization, the insider made several product demonstrations to various foreign agents and customers using the information he stole. During several of the presentations, the insider slightly modified the stolen intellectual property to make it appear as though his new foreign employer developed it. The insider was eventually arrested when an individual at one of the insider's demonstrations noticed that the product he was displaying belonged to the victim organization and notified the authorities. He was convicted, but the case material does not state whether the IP was returned to the victim organization or recovered from the foreign competitor.
4. The insider worked as a researcher at a manufacturing company for over ten years. Two months before leaving the victim organization, he signed an agreement to start working for a foreign competitor. However, he did not inform the victim organization that he would be working for a competitor until just a few weeks prior to his scheduled departure. During the two months before his departure, he accessed the victim organization's database of proprietary and confidential information and downloaded thousands of documents--more than ten times the amount of the next-highest user. The insider was able to access information wholly unrelated to his research responsibilities, including R&D projects he had no role in developing. The insider also stole so much paper that he had to obtain extra storage space at his residence. The total value of the stolen information was in the range of several hundred million dollars. Only after the insider announced his employment with a competitor did the victim organization begin to investigate the excessive downloads and alert the authorities. At the new employer, the insider was in the process of transferring the stolen data to one of its company-issued laptops when the authorities asked the new employer to seize the computer. The investigation of the insider's home uncovered the massive amounts of paper files that the insider was in the process of destroying and computer hard drives he attempted to delete. The insider was convicted and the new employer cooperated with the authorities by returning the IP.
5. The insider worked as an engineer at a semiconductor manufacturing plant. Several months before he left the victim organization, he used his company desktop to download and email proprietary data sheets to a foreign organization. The information transferred was beyond what was required for his duties, but he was still able to access it. Several employees noticed that he had downloaded information prior to leaving, but he maintained that the victim organization did not prohibit downloading information to private spaces to facilitate productivity. He resigned from the victim organization without informing them he had already accepted a position with a foreign competitor. During the exit interview, the victim company reminded the insider that he had signed an intellectual property agreement, but that had no impact on the insider's malicious actions. Only after he sent his letter of resignation did two of his coworkers inform management about the insider's downloads. Based on that report, the victim organization sought the services of an

external forensic company to investigate the insider's activity. The forensic examination revealed that the insider had indeed used company hardware and his personal email account to send the data sheets to the foreign competitor. The examination also revealed that the insider held several instant message conversations with executives at the foreign organization while at work, on company equipment. The insider was convicted, and the victim organization did not believe that the disclosure of the IP materially affected their business operations.

6. The insiders worked as post-doctoral research fellows. While still employed by the victim organization, the insiders accepted a position with another domestic institution. They also agreed to collaborate with a foreign company to develop products based on stolen information. One of the insiders had sent an email to the foreign company agreeing to collaborate with them. Despite signing intellectual property agreements, and the lab area being considered physically secure, they were able to steal proprietary information that included their research data and boxes of physical goods such as lab materials, books, and documents. The organization detected the theft through reports by another employee who noticed the large amount of material that was missing from the lab area. The charges were dropped against both insiders since there was insufficient evidence to support the claim that the stolen information was proprietary.

Summary of Case Details

Table 1 summarizes some of the pertinent details related to the cases included in this article.

Detail	1	2	3	4	5	6	7	8	9	10
Subject:										
Scientist/Computer Engineer	x	x	x	x	x	x	x	x	x	x
Naturalized U.S. Citizen		x		x	x	x		x		
Foreign National			x				x		x	x
Target:										
Format: Electronic	x	x	x	x	x	x	x	x	x	x
Format: Physical	x		x	x	x				x	x
Type: Source Code		x	x		x		x			
Type: Product Information	x	x		x		x		x	x	
Type: Research Materials										x
Information Outside of Job Scope					x			x	x	
Incident:										
Location: On Site	x	x	x	x	x		x	x	x	x
Location: Remote Access					x					
Time: During Normal Business Hours		x	x	x	x		x	x	x	
Time: Outside Normal Business Hours					x					x

Table 1 - Detailed Case Summary

Recommendations for Mitigation and Detection

Summary of Recommendations

This article focuses on cases that involve foreign governments or organizations because of the increased potential impact. However, all theft of IP cases share similar enough patterns that risk mitigation strategies should be effective regardless of foreign involvement.

Organizations need to assess the potential consequences of an insider successfully stealing proprietary company information and implement strategies commensurate with that potential impact. Cost-effective strategies require an organization to determine its most valuable assets and balance the effort and funding dedicated to protecting those assets with the potential impact of their loss. Although the following recommendations are not foolproof, they can be an effective addition to the defense-in-depth strategy and potentially deter a less motivated attacker or detect one who does take action. Table 2 contains a summary of these recommendations as they relate to the cases.

Recommendation 1: *Establish an employee exit procedure.* Organizations should maintain logs of critical file access and physical access for at least a one-month timeframe for all employees. Our research shows that most employees who steal intellectual property commit the theft within one month of resignation. In the event an employee resigns, whether unexpectedly or not, a previously designated individual should audit and review these logs for any suspicious activity. Moreover, organizations should develop and clearly document the employee termination process that includes, but is not limited to, the following items:

- Remind the departing employee of any IP agreement that he or she may have signed at the organization and have him or her sign it once more.
- Ensure that the employee has returned all company property, whether it be electronic or paper documents, hardware, or software.

Organizations should remind all employees of their contractual obligations when terminating their employment. This may facilitate prosecution and show that the organization has exercised due diligence. More specifically, organizations should remind employees at their exit interview that they are required to return all company property, and consider not allowing employees to vacate the premises until they have done so.

Recommendation 2: *Monitor intellectual property leaving the network.* First, organizations need to identify critical information and track where it is located. Organizations should also consider implementing mechanisms that log critical information that employees

- download from company servers
- email off of the network, particularly to competitors, outside the U.S, and to personal email accounts like Gmail or Hotmail
- download to removable media

Organizations should investigate suspicious transactions, particularly upon employee resignation. As seen in the cases, the time immediately preceding termination is an especially critical period for monitoring. Many of the cases involved insiders downloading source code, executables, or excessive amounts of data prior to leaving the organization. Examining the logs could aid the detection of proprietary data exfiltration and mitigate the risk of IP theft.

Recommendation 3: *Maintain adequate physical security.* Although much of an organization's proprietary information most likely is stored in digital formats, it is still crucial to maintain physical security. As seen in the cases, insiders stole physical assets such as printed documents, datasheets, and hardware. One potential mitigation strategy is to monitor the frequency and volume of printouts that employees make of proprietary information. If the employee exceeds a predetermined threshold or deviates from his or her normal pattern of behavior, then the organization could perform a more in-depth audit of the employee's activities. Several cases did involve insiders stealing somewhat large amounts of physical property, such as large containers of physical documents, research materials, or physical hardware components.

Recommendation 4: *Institute the principle of least privilege.* Although employees need legitimate access to some intellectual property as a function of their employment, users should not have unfettered access to all of a company's proprietary information. In several cases, the insider was able to access information that should have been restricted on a "need to know" basis. Institute the principle of least privilege and reduce the access of employees to only include information that pertains to their current assignment. If an employee's assignment requires escalated privileges, then the organization should revoke those privileges when the employee no longer works on that assignment. Co-workers should also be aware that excessive, or uncharacteristic, interest in areas outside an employee's area of responsibility may be an indication of an insider threat. All employees should have anonymous methods to report such suspicious behavior.

Table 2 displays the recommendations and the applicability of each to the cases.

Recommendation	1	2	3	4	5	6	7	8	9	10
1 - Establish an employee exit procedure					x	x	x	x	x	x
2 - Monitor IP leaving the network	x	x	x		x		x	x	x	
3 - Maintain adequate physical security			x	x	x				x	x
4 - Institute the principle of least privilege					x			x	x	

Table 2 –Recommendation Applicability to Cases

The problem of insider theft of intellectual property is difficult to manage because employees need some level of access to proprietary information in order to do their jobs. However, by following the recommendations outlined in this article, organizations can attempt to minimize the potential impact of an insider theft of IP incident. Some of the attacks in the cases could have been, and in some cases were indeed, prevented or quickly detected using some combination of the proposed recommendations.

About the Insider Threat Team

The Insider Threat team is part of the Threat and Incident Management (TAIM) team in CERT. The TAIM team helps organizations improve their security posture and incident response capability by researching technical threat areas; developing information security assessment methods and techniques; and providing information, solutions, and training for preventing, detecting, and responding to illicit activity. TAIM team members are domain experts in insider threat and incident response, and team capabilities include threat analysis and modeling; development of security metrics and assessment methodologies; and creation and delivery of training, courses, and workshops. Our insider threat database allows us to examine broad and specific trends.

For additional information regarding the content of this article or other research conducted at The Insider Threat Center at CERT, please contact Dawn Cappelli (dmc@cert.org).