Software Engineering Institute

Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations

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

May 2013

TECHNICAL NOTE
CMU/SEI-2013-TN-009

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon

Copyright 2013 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense. This report was prepared for the

SEI Administrative Agent
AFLCMC/PZE
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon®, CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM-0000217

Table of Contents

Acknowledgements **v**

Abstract **vii**

1 Introduction **1**

2 Snapshot of the Insiders **2**

2.1 Who They Are 3

2.2 What They Stole and the Impact on the Business 4

2.3 Where and When They Steal 5

2.4 Why They Steal 5

2.4.1 Externally Influenced Theft of IP 6

2.4.2 Internally Influenced Theft of IP 6

2.5 How They Steal 6

3 Summary of Cases **8**

3.1 Externally Influenced Theft of Intellectual Property 8

3.2 Internally Influenced Theft of Intellectual Property 9

4 Recommendations for Mitigation and Detection **11**

4.1 General Recommendations 11

Recommendation 1: Establish an employee exit procedure. 11

Recommendation 2: Monitor intellectual property leaving the network. 11

Recommendation 3: Maintain adequate physical security. 12

Recommendation 4: Consider enforcing least-privilege access. 12

Recommendation 5: Monitor communications with competitors. 12

4.2 Specific Recommendations for Foreign Travel and International Companies 13

Recommendation 6: Institute policies and best practices for foreign travel. 13

Recommendation 7: Audit supplier bids to detect anomalies. 13

5 Summary **14**

6 About the Insider Threat Team **15**

References **17**

List of Figures

Figure 1: Summary Statistics for IP–FB Cases, by Number of Cases 3

Figure 2: Types of Insider, by Number of Cases 4

Figure 3: Time of Insider Theft of IP, by Number of Cases (Excludes the Nine Cases in Which the Time Was Unknown) 5

Figure 4: Internally or Externally Influenced Theft of IP, by Number of Cases 6

Acknowledgements

Special thanks to Paul Ruggiero and all of the Software Engineering Institute's CERT® Division.

Abstract

This is the sixth entry in the *Spotlight On* series published by the CERT® Insider Threat Center. Each entry focuses on a specific area of threat to organizations from their current or former employees, contractors, or business partners and presents analysis based on hundreds of actual insider threat cases cataloged in the CERT insider threat database. This entry in the series focuses on insiders 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. This technical note defines IP and insider theft of IP, explains the criteria used to select cases for this examination, gives a snapshot of the insiders involved in these cases, and summarizes some of the cases themselves. Finally, it provides recommendations for mitigating the risk of similar incidents of insider threat.

1 Introduction

This technical note is an update of a 2009 article, funded by CyLab, from the series *Spotlight On*, published by the Insider Threat Center at the CERT® Division, part of Carnegie Mellon University's Software Engineering Institute (SEI). Each entry in the *Spotlight On* series focuses on a specific area of insider threat and presents analysis based on hundreds of actual insider threat cases cataloged in the CERT insider threat database. For more information about the CERT Division's insider threat work, see http://www.cert.org/insider_threat/.

In this technical note, we focus on current or former employees, contractors, or business partners who used information technology (IT) to steal intellectual property (IP), such as source code, scientific formulas, engineering drawings, strategic plans, or proposals, from their organizations to benefit a foreign entity.

Some of the cases examined for this technical note involved more than one insider working together against the victim organization. These cases give us insight into the details of insider attacks conducted for a foreign entity, including their potential damage to victim organizations. Our research shows that insider theft of IP for the benefit of a foreign organization is, on average, four times more costly to the victim than insider theft of IP that benefits a domestic organization [Cappelli 2012].

The CERT Division defines IP and insider theft of IP as the following [Cappelli 2012]:

- intellectual property: "Intangible assets created and owned by an organization that are critical to achieving its mission."
- insider theft of intellectual property: "An insider's use of IT to steal proprietary information from the organization. This category includes industrial espionage involving insiders."

We drew the cases examined for this technical note from the CERT insider threat database, which catalogs more than 700 cases of insider threat reported in court documents, U.S. Department of Justice press releases, and the media. We did not include cases of theft of U.S. government classified or export-controlled information. To be included in this examination, cases had to meet three conditions: (1) the insider used IT to steal IP from the victim organization, (2) the victim organization was located in the United States, and (3) the beneficiary organization was located in a country outside the United States. We found 29 such IP–foreign beneficiary (IP–FB) cases that met the requirements for inclusion in this examination.

The next section of this technical note describes insiders who used IT to steal IP for a foreign entity, focusing on the questions of *who*, *what*, *where*, *when*, *why*, and *how*. Section 3 summarizes the relevant details of the IP–FB cases. Section 4 lists recommendations for mitigating the risk of similar occurrences.

® CERT® is a registered mark owned by Carnegie Mellon University.

2 Snapshot of the Insiders

The majority of the 29 IP–FB cases fit the problem described in *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, prepared by the Office of the National Counterintelligence Executive [ONCIX 2011]:

> *Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security. Cyberspace—where most business activity and development of new ideas now takes place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect.*

In all of the IP–FB cases, malicious insiders misused a company's systems, data, or network to steal IP from an organization inside the United States for the benefit of a foreign entity. Each entity was either an existing foreign organization or a new company that the insiders established in a foreign country. The cases also involved activities defined by the Office of the National Counterintelligence Executive as economic espionage or industrial espionage [ONCIX 2011]:

> *Economic espionage occurs when an actor, knowing or intending that his or her actions will benefit any foreign government, instrumentality or agent, knowingly: (1) steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1831).*
>
> *Industrial espionage, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmitting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1832).*

The IP–FB cases do not include the theft or modification of personally identifiable information (PII) or credit card information. Our insider threat research has determined that those who steal IP—ambitious leaders and entitled independents—typically do not steal PII or credit card information [Moore 2011].

Cases that involve foreign beneficiaries can differ from other cases of theft of IP because the insiders may have a sense of duty or loyalty to their countries of birth that overrides any loyalty to their employer. Moreover, some of these cases suggest that some foreign entities assist insiders who steal IP to advance businesses in that particular country. Competing loyalties, coupled with

the influence of foreign nations or organizations on insiders in the United States, 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. Limiting the damage from a crime that extends outside the jurisdiction of U.S. law enforcement can be more difficult for an organization than limiting damage from a domestic crime. Insiders who leave the United States may be difficult or impossible to locate and arrest. Even insiders who are located and arrested have to be extradited to the United States. In addition, it can be very difficult to recover stolen IP once it leaves the United States. Within U.S. borders, a company that receives and uses stolen IP for their own advantage is subject to the same laws and consequences as the insiders who stole it, so domestic organizations have a greater obligation than foreign organizations to cooperate with authorities and return all stolen IP.

Figure 1 breaks down the cases used for this technical note. The following sections give more detailed information on these categories.

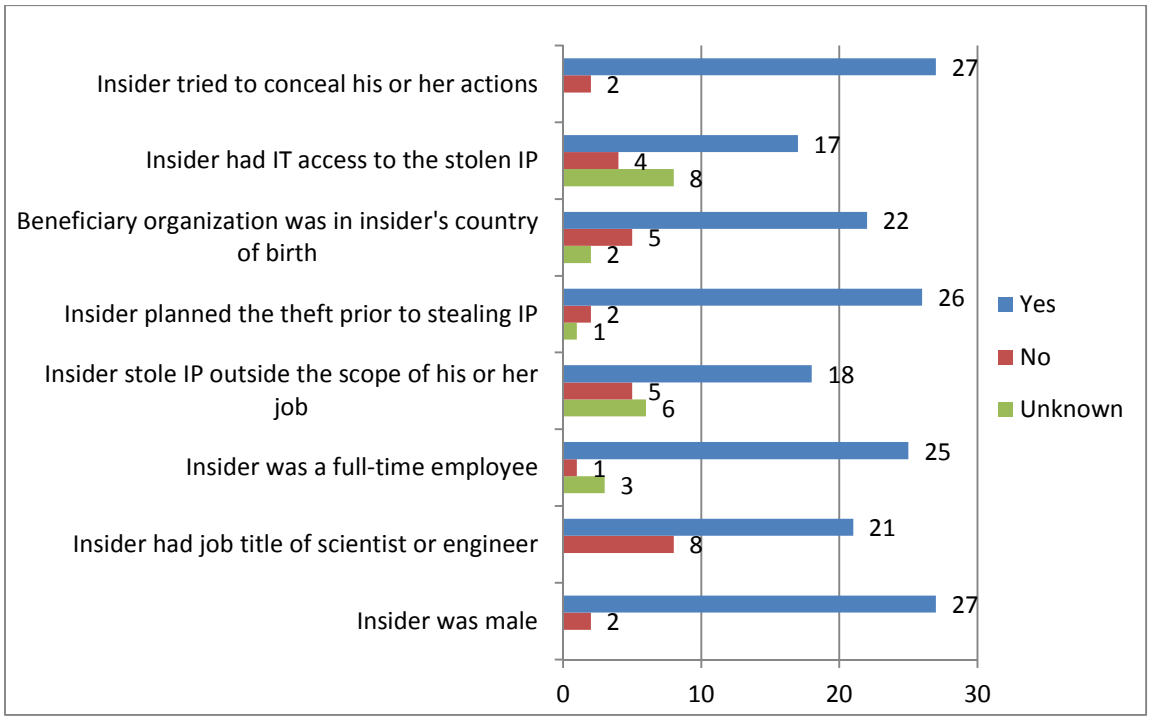

Figure 1: Summary Statistics for IP–FB Cases, by Number of Cases

2.1 Who They Are

Of the 29 IP–FB cases, 27 involved male insiders. Insiders sought to benefit an organization or government located in their country of birth in 22 of the 29 cases.

The majority of insiders in the IP–FB cases held technical positions: more than 70% of the insiders were scientists or engineers. This is significantly different from the cases of IP theft that benefit domestic organizations, in which scientists and engineers represent 21% of insiders who steal IP for the benefit of a domestic organization.

Of the 29 IP–FB cases, 25 involved insiders who worked full time, 1 involved an insider who worked as a contractor, and 3 involved insiders whose job status was unknown. The majority of the insiders stole IP related to their work. The insiders from 10 of the cases had a job title that included the word "senior" or "manager," indicating that insider threats exist throughout the organization.

Recent research conducted at the CERT Division identified two profiles of insiders who stole IP [Moore 2011]:

- entitled independent: an insider acting primarily alone to steal information to take to a new job or to his own side business
- ambitious leader: a leader of an insider crime who recruits insiders to steal information for some larger purpose

We found that the majority of insiders in IP–FB cases fell into the ambitious leader model (see Figure 2). Foreign entities can influence these insiders in a way that makes the insider feel he or she is contributing to some larger cause, including the benefit of a foreign organization or government. Though it is not necessary for further understanding of this paper, more information on the two profiles of insiders and on the insider theft of IP can be found in the publication *A Preliminary Model of Insider Theft of Intellectual Property* [Moore 2011].

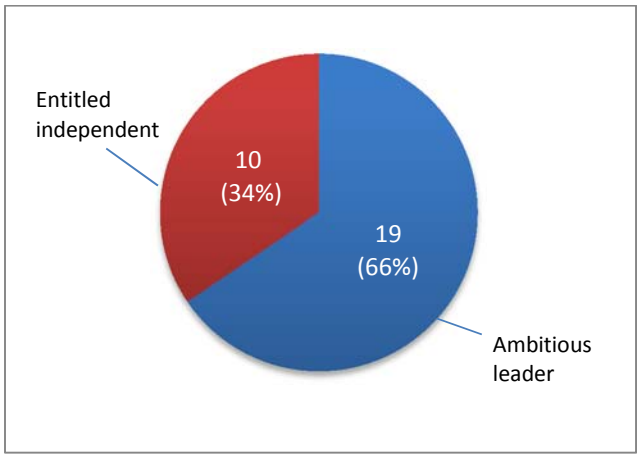

Figure 2: Types of Insider, by Number of Cases

2.2 What They Stole and the Impact on the Business

Insiders in five of the cases stole IP strictly related to their jobs. Eighteen cases involved insiders who stole IP related to their jobs and IP outside the scope of their jobs. It is unknown whether the insiders in the remaining six cases stole IP within or outside the scope of their jobs.

The thefts had a wide range of impacts on the victim organizations, some of which include

- decreased sales of a product in a foreign country after a competitor there used information from an insider to make a competing product
- loss of more than $1,000,000 in sales revenue
- damage to the organization estimated to exceed $100,000,000 in two cases
- loss of more than $40,000,000 in documents

- loss of a formula that cost over half a billion dollars in research and development
- loss of competitive advantage
- bankruptcy

2.3 Where and When They Steal

Of the 29 IP–FB cases, 14 involved insiders who stole IP only during working hours, 5 involved insiders who stole IP during both working and nonworking hours, and 1 involved an insider who stole IP only outside of working hours (see Figure 3). It is unknown whether the insiders in the remaining 9 cases stole IP during working or nonworking hours. Insiders involved in 26 of the cases planned their removal of IP prior to the theft. Two cases involved insiders who did not have plans to remove the IP before they stole from the organization, and the insider's plans from one case are unknown. The majority of the IP–FB insiders committed their theft while working at the victim organization, but shortly before resigning or taking another position. Two cases involved insiders who had one-way travel tickets to the country of the beneficiary organization and were caught after they were searched at the airport.

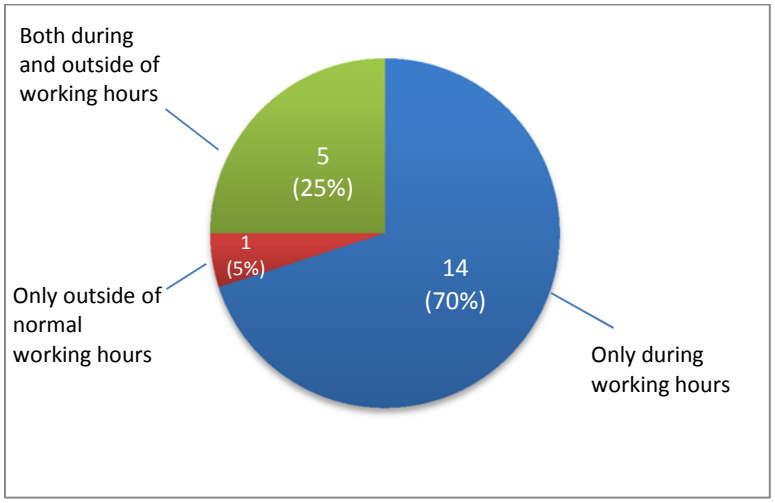

Figure 3: Time of Insider Theft of IP, by Number of Cases (Excludes the Nine Cases in Which the Time Was Unknown)

2.4 Why They Steal

Nearly all of the IP–FB insiders stole IP to gain a business advantage for a competitor or to create a new business. The extent to which the beneficiary organization is involved in the theft of IP reveals influences on the insider's actions. The 29 IP–FB cases fell into two categories of influence: external and internal (see Figure 4). Cases in which the degree of external influence was not clear but there was some communication between the insider and the beneficiary organization were classified as externally influenced.

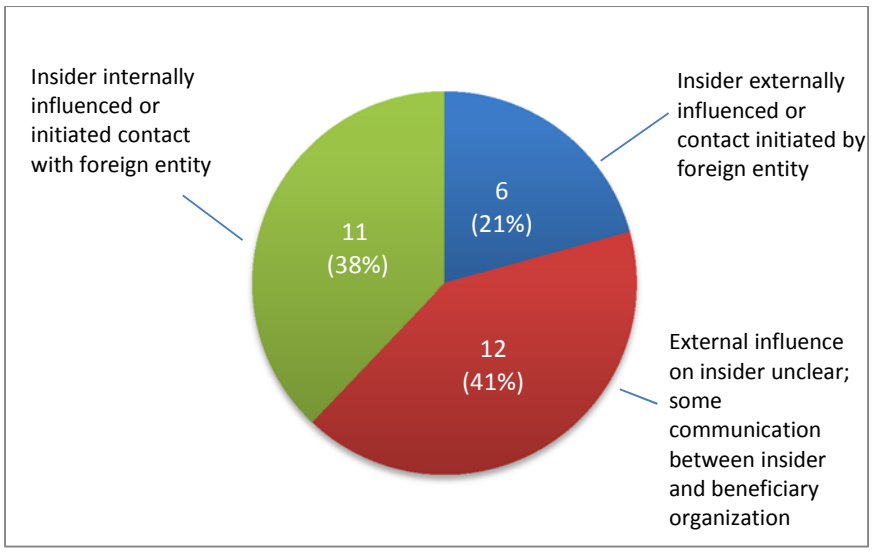

Figure 4: Internally or Externally Influenced Theft of IP, by Number of Cases

2.4.1 Externally Influenced Theft of IP

In the 18 externally influenced cases of IP–FB, foreign organizations played a role in the theft of IP or were aware of the insider's actions. In 6 of these cases, foreign organizations heavily influenced the insiders by initiating contact and providing the insider funding or technical means to steal IP. In the remaining 12 externally influenced cases, it is unclear whether the insiders or the foreign organizations initiated contact, but the foreign organizations were aware of the insiders' actions in some way. In 16 of the 18 cases, the insiders stole IP for foreign organizations located in the insiders' country of birth. The insiders in all of the externally influenced cases fit the ambitious leader profile, and two of the insiders had close ties to the country where the beneficiary organization was located. None of these cases involved insiders born in the United States.

2.4.2 Internally Influenced Theft of IP

In the 11 internally influenced IP–FB cases, the insider contacted the foreign organization with an offer, in hopes of personal gain or a new job, and received no apparent assistance from the beneficiary organization in the theft of IP. In 9 of these cases, the insiders fit the entitled independent profile. Insiders stole IP for the benefit of a foreign organization in their country of birth in only 5 of the 11 internally influenced cases. Only 2 of the 11 cases involved internally influenced insiders born in the United States.

2.5 How They Steal

Insiders tended to use authorized means to steal IP. In cases in which the method of theft is known, no insiders used malicious code or exploited a technical vulnerability to perpetrate their thefts. The level of IT authorization for the insiders is known for 21 of the 29 IP–FB cases. Of these 21 cases, 17 included insiders who had authorized IT access. Eleven of these 17 cases involved insiders with authorized IT access to the stolen IP. In 6 of these 17 cases, insiders had authorized IT accounts but did not have permission to view the stolen IP. In 4 of the 21 cases for which IT authorization is known, the insiders did not have any authorized IT access. These

insiders bribed other employees, stole other employees' credentials, and used social engineering to obtain the stolen IP.

The insiders used methods such as

- accessing the company's internal servers, either on-site or using virtual private network (VPN) and copying the information to their computers or 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 outside of 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 more than 20 boxes of physical research material from a supposedly secure environment.
- emailing information out of the organization using a personal email account on a company computer

Of the 29 IP–FB cases, 27 cases involved insiders who tried to conceal their actions by, for example, lying on exit interviews, logging in with other users' credentials, and deleting files to cover their tracks.

3 Summary of Cases

Summaries of six of the IP–FB cases follow, divided into externally influenced and internally influenced cases.

3.1 Externally Influenced Theft of Intellectual Property

1. A senior research engineer worked for the victim organization, a manufacturing organization. Due to the insider's experience, an external third party asked the insider to lecture in his country of birth. While on this trip, the beneficiary organization offered the insider a position as a consultant. For a period greater than five years, the beneficiary organization paid the insider more than $150,000 to provide the victim organization's trade secrets. The insider used email and faxes to remove the data from the organization and had payments sent to relatives to conceal his actions. The victim organization discovered the insider theft after interviewing a former worker of the beneficiary organization for a position. The insider was subsequently arrested, convicted, and sentenced to probation and home detention. The beneficiary organization was fined more than $4 million. The total value of the trade secrets is estimated to be greater than $45 million.
2. The insider, a naturalized U.S. citizen, was employed as a senior research and development associate by the victim organization, a manufacturer. The insider was disgruntled and took advantage of the opportunity to work with three executives from a competing foreign organization, located in the insider's country of birth. The insider made more than 15 trips to exchange the victim organization's IP, stored on external storage devices, for cash payments. The beneficiary organization also covered the insider's travel expenses. To avoid detection, the insider pretended to be a consultant for the beneficiary organization. The insider was caught when the beneficiary organization advanced their technology too quickly and an employee at the victim organization reported a suspected insider. The insider was arrested, convicted, ordered to pay restitution, and sentenced to over a year in prison.
3. The insider worked as a chemist and later a product development director at a manufacturing plant. He made a business trip abroad to work with one of the victim organization's subsidiaries, and a co-worker 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 had no legitimate reason to possess. The authorities also noticed that the insider's LinkedIn profile stated that he was now employed by a competitor in a foreign nation. The insider was arrested, convicted, and sentenced to over one year in prison followed by supervised release. The insider was also ordered to pay restitution.

3.2 Internally Influenced Theft of Intellectual Property

1. 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 start-up that supposedly served a similar but unique market niche. The two insiders used this start-up company to develop a prototype for a telecom device based almost entirely on the proprietary information stolen from their previous employer. These individuals met with a consultant to obtain venture capital; however, they refused to show a prototype to the consultant 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. The insiders stole hardware components and exfiltrated proprietary information by email while still employed by the telecommunications firm. They then stored the information on their start-up company's password-protected website to make it available to their foreign business partner. The individuals also made several trips to the foreign company to finalize the joint venture.

   The insiders used several methods to disguise their activity and conceal their association with the start-up company:

   - 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 start-up company
   - removing their names from the internet registry of their start-up company's website
   - using aliases (and obtaining business cards for these aliases) for all public communication regarding the start-up company

   Investigators uncovered a great deal of proprietary information in one insider's basement, including 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 and the financial impact on the victim organization remain unknown.

2. The lead insider and an accomplice worked as engineers at victim organizations in the United States. The lead insider was employed at two victim organizations, and the accomplice was employed at two other victim organizations. The two insiders stole IP from the four victim organizations 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 time frame 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. The insiders were arrested, convicted, and sent to prison for almost two years.

3. The insider was a product engineer at the victim organization, an automobile manufacturer. Due to the nature of the insider's work, the insider had access to trade secrets and design specifications from the company. Nearly two years prior to leaving the organization, the insider downloaded design specifications and used them to aid in finding employment at competing organizations. A year and a half after stealing the design specifications, the insider accepted a job offer from a company that manufactured automotive electronics in a

foreign country. The insider continued to work at the victim organization for two months after accepting this job offer. The night before permanently leaving the victim organization, the insider downloaded thousands of documents onto an external hard drive. These documents included company designs for various automotive systems and were valued at more than $20 million. The majority of these documents were unrelated to the insider's job at the victim organization.

The insider traveled to the foreign country to work for the beneficiary organization and did not submit a letter of resignation to the victim organization until two weeks later. One year after leaving the victim organization, the insider was hired by a direct competitor of the victim organization located in the same foreign country as the first beneficiary organization. The insider was arrested upon returning to the United States. Forensic examiners examined the insider's laptop and found thousands of confidential and proprietary documents from the victim organization. The insider was arrested, convicted, and sentenced to over five years in prison.

4 Recommendations for Mitigation and Detection

This technical note focuses on cases that involve foreign governments or organizations because of the increased potential impact of IP exfiltration outside of the United States. However, all IP theft cases share similar enough patterns that risk mitigation strategies should be effective whether or not the case involves foreign entities.

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, potentially deterring a less motivated attacker or detecting one who does take action.

4.1 General Recommendations

Recommendation 1: Establish an employee exit procedure.

Organizations should develop and clearly document an 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 signed at the organization and have the employee sign it once more.
- Ensure that the employee has returned all company property, whether it is electronic or paper documents, hardware, or software.

Organizations should remind all employees of their contractual obligations surrounding termination. This may facilitate prosecution and show that the organization has exercised due diligence. When applicable, organizations should require employees to sign a nondisclosure agreement and a noncompete agreement upon separation from the organization. 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.

In addition to establishing an employee exit procedure, organizations should maintain logs of critical file access and physical access for at least a one-month time frame for all employees. Our research shows that most employees who steal IP commit the theft within 30 days before or after leaving the organization. When an employee resigns, whether unexpectedly or not, a previously designated individual should audit and review these logs for any suspicious activity. Organizations need to identify critical information and track its location, access, modifications, and transfers. Organizations should also consider implementing technical controls that log the movement of critical information that employees

- download from company servers

- email from the organization's network to competitors, including those outside the United States, and to personal email accounts
- download to removable media

Many of the cases involved insiders downloading source code, executables, or excessive amounts of data prior to leaving the organization. Examining logs and monitoring intellectual property leaving the network may enable detection of proprietary data exfiltration, further mitigating 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. Our case data shows that 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 involved insiders stealing large amounts of physical property, such as large containers of physical documents, research materials, or physical hardware components.

Recommendation 4: Consider enforcing least-privilege access.

Although employees need legitimate access to some IP as a function of their employment, users should not have unfettered access to all of a company's proprietary information. In at least 14 of the cases, the insider was able to access information that should have been restricted via technical controls on a need-to-know basis. Organizations should consider the principle of least privilege and reduce the access of employees to include only 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 be able to anonymously report such suspicious behavior. Use of technical controls, including regular audits and updates of file permissions, enforces policy and limits employee access to IP outside the scope of their work.

Recommendation 5: Monitor communications with competitors.

Employers should consider requiring employees to report any business offers from competitors, both domestic and foreign. Employees should report all consulting work to a central authority for review for conflicts of interest and approval. Organizations should use technical controls to monitor incoming and outgoing email for communications with competing organizations. A system should be set up to flag and review any email to or from a competitor.

4.2 Specific Recommendations for Foreign Travel and International Companies

Recommendation 6: Institute policies and best practices for foreign travel.

Scientists, engineers, those in research and development, and other employees with access to a significant amount of IP should be required to notify the organization of any foreign travel. Organizations should implement a strict policy to prevent the organization's electronics and electronic files from leaving the country, except for official use. When an employee must take a laptop abroad, the organization should provide a laptop that is approved for foreign travel and contains only the documents necessary for the trip. Before the employee departs, the organization should review any information the employee will present to ensure it is acceptable. Organizations should brief employees regarding acceptable contact with foreign organizations. Upon an employee's return to the organization, the employee should report any contact with foreign organizations. Regardless of whether the employee reports foreign contact, the organization should act based on the assumption that foreign entities have compromised the employee's personal electronics. The travel laptop should not be connected to internal networks and should be securely wiped after each trip. To further minimize the chance of data exfiltration, organizations should disable USB ports and CD burners if they are not required for the employee's job.

Recommendation 7: Audit supplier bids to detect anomalies.

In some of the IP–FB cases, insiders initiated contact with foreign suppliers to make deals. In addition to passing along trade secrets, insiders would tell foreign suppliers the bids of other suppliers to help the foreign suppliers win the project. These employees could circumvent technical controls because access to bidding information was required for their job. Organizations should routinely review the bids of suppliers to determine if one company consistently underbids the competition by a small margin. This may be a sign of an insider divulging information to suppliers.

5 Summary

The problem of insider theft of IP is difficult to manage because employees need some level of access to proprietary information to do their jobs. However, by following the recommendations outlined in this technical note, organizations can attempt to minimize the potential impact of an insider theft of IP. Implementing the proposed recommendations may have prevented or led to the earlier detection of the majority of the examined IP–FB attacks. A combination of clearly communicated policies and technical controls can help mitigate the risk of insider theft of IP for the benefit of a foreign organization.

6 About the Insider Threat Team

The CERT Insider Threat Center is part of the Enterprise Threat and Vulnerability Management (ETVM) team in the CERT Division. The ETVM 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 insider activity. ETVM 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 technical note or other research conducted at the CERT Insider Threat Center, please contact insider-threat-feedback@cert.org.

References

URLs are valid as of the publication date of this document.

[Cappelli 2012]

Cappelli, D.; Moore, A. P.; & Trzeciak, R. F. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley, 2012. http://www.sei.cmu.edu/library/abstracts/books/9780321812575.cfm

[Moore 2011]

Moore, A. P.; Cappelli, D. M.; Caron, T.; Shaw, E.; Spooner, D.; & Trzeciak, R. F. *A Preliminary Model of Insider Theft of Intellectual Property* (CMU/SEI-2011-TN-013). Software Engineering Institute, Carnegie Mellon University, 2011. http://www.sei.cmu.edu/library/abstracts/reports/11tn013.cfm

[ONCIX 2011]

Office of the National Counterintelligence Executive. *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*. Office of the Director of National Intelligence, 2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. **AGENCY USE ONLY** (Leave Blank)	2. **REPORT DATE** May 2013	3. **REPORT TYPE AND DATES COVERED** Final
4. **TITLE AND SUBTITLE** Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations		5. **FUNDING NUMBERS** FA8721-05-C-0003
6. **AUTHOR(S)** Matthew L. Collins, Derrick Spooner, Dawn M. Cappelli, Andrew P. Moore, Randall F. Trzeciak		
7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. **PERFORMING ORGANIZATION REPORT NUMBER** CMU/SEI-2013-TN-009
9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)** HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116		10. **SPONSORING/MONITORING AGENCY REPORT NUMBER** n/a
11. **SUPPLEMENTARY NOTES**		
12A **DISTRIBUTION/AVAILABILITY STATEMENT** Unclassified/Unlimited, DTIC, NTIS		12B **DISTRIBUTION CODE**

13. **ABSTRACT (MAXIMUM 200 WORDS)**

This is the sixth entry in the Spotlight On series published by the CERT®Insider Threat Center. Each entry focuses on a specific area of threat to organizations from their current or former employees, contractors, or business partners and presents analysis based on hundreds of actual insider threat cases cataloged in the CERT insider threat database. This entry in the series focuses on insiders 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. This technical note defines IP and insider theft of IP, explains the criteria used to select cases for this examination, gives a snapshot of the insiders involved in these cases, and summarizes some of the cases themselves. Finally, it provides recommendations for mitigating the risk of similar incidents of insider threat.

14. **SUBJECT TERMS** insider threat, intellectual property, IP, foreign, economic espionage, industrial espionage, security, information security, information assurance, cybersecurity	15. **NUMBER OF PAGES** 29
16. **PRICE CODE**	

17. **SECURITY CLASSIFICATION OF REPORT** Unclassified	18. **SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	19. **SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	20. **LIMITATION OF ABSTRACT** UL