CERT

Spotlight On: Insider Threat from Trusted Business Partners

February 2010

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

This work was funded by

CyLab
www.cylab.cmu.edu

Software Engineering Institute | Carnegie Mellon

Spotlight On: Insider Threat from Trusted Business Partner

This report is the fourth 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/.

This article will focus on cases in which the insider was employed by a trusted business partner of the victim organization. We first define the concept of trusted business partner (TBP) and then describe case scenarios in which a TBP has become an insider threat. These case scenarios concentrate on presenting the *who*, *what*, *why*, and *how* of the illicit activity. Finally, we provide recommendations that may be useful in countering these threats.

We would like to thank the following for their contributions to this article: Sally Cunningham - Deputy Director of Program, Development, and Transition at the SEI; William Shore - retired Special Agent with the FBI who is now the Manager of Security at the Software Engineering Institute; and Dr. Eric Shaw – a visiting scientist at CERT and clinical psychologist at Consulting & Clinical Psychology, Ltd.

Snapshot of Insider Threat from Trusted Business Partners

What is a Trusted Business Partner?

For the purposes of this article, a ***TBP*** is defined as any external organization or individual an organization has contracted to perform a service for the organization. The nature of this service requires the organization to provide the TBP authorized access to proprietary data, critical files, and/or internal infrastructure. For example, if an organization creates a contract with an outside organization to perform billing services, it would have to provide access to its customer data, thereby establishing a trusted business partnership. However, the TBP concept does not include cases in which the organization is simply a customer of another company. For example, when an organization uses a bank, it is simply a client of the bank. This customer-vendor relationship would not be considered a TBP relationship.

This definition includes two different types of relationships between the organization and the TBP. An ***organizational relationship*** is one in which one organization outsources a service to a TBP. For example, an organization outsourcing its customer helpdesk support service to an outside company has entered into a TBP relationship with that company. In this case, the organization must grant access to its customer database to the outside organization.

In contrast, some employees working for a TBP could have an individual relationship with the victim organization. An ***individual relationship*** includes individual consultants, temporary employees, and contracted employees. An ***individual consultant*** is an individual who performs services for the organization, but who is not an employee of the organization. This includes any employees who have terminated their employment with an organization and who are then hired on as a consultant. A ***contracted employee*** is any employee hired under a contractual agreement between an organization and a contract organization (the TBP). The contracted employee works full time for the organization, but receives compensation through the TBP. A ***temporary employee*** is any person hired for a short period of time to fill in for an employee who has left or is on leave.

Overview of Insiders from TBP

According to a recent study by the security companies RSA and Interactive Data Corporation (IDC) which surveyed C-level executives, "Contractors and temporary staff represent the greatest internal risk [to] organizations."[1] However, of the more than 300 cases in our database, only 34 were committed by contractors or temporary staff, accounting for roughly 10 percent of all cases. (An additional 11 cases involved employees of companies providing an outsourced service.) So, while the RSA/ICS survey indicates the problem of attacks by contractors and temporary staff is of high concern to the C-level executives surveyed, our data indicate individuals employed directly by an organization were more often the perpetrators of insider crimes than were contractors or temporary staff.

TBP insider cases occurred in a number of industry sectors. For example, while a greater number of cases occurred in the government and information technology sectors, cases were also observed in the financial, medical, education, entertainment, manufacturing, and utility sectors. Figure 1 below displays the breakdown of cases by industry according to the cases in CERT insider threat database.

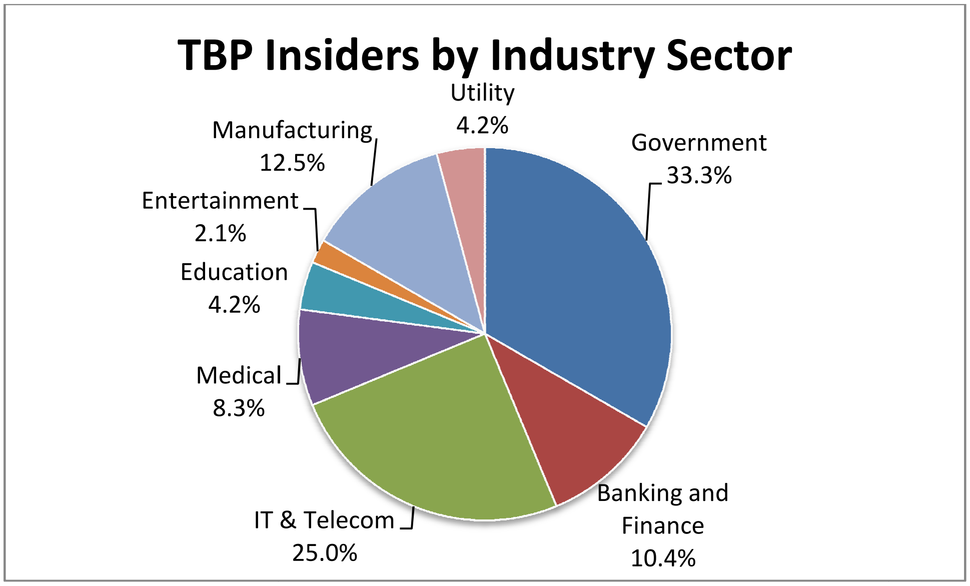

Figure 1 - TBP Insiders by Industry Sector

Of the total forty-five cases, eleven had an organizational relationship and the remaining thirty-four had an individual relationship with the victim organization. Figure 2 presents TBP-related cases by type.

[1] See http://www.rsa.com/solutions/business/insider_risk/wp/10388_219105.pdf

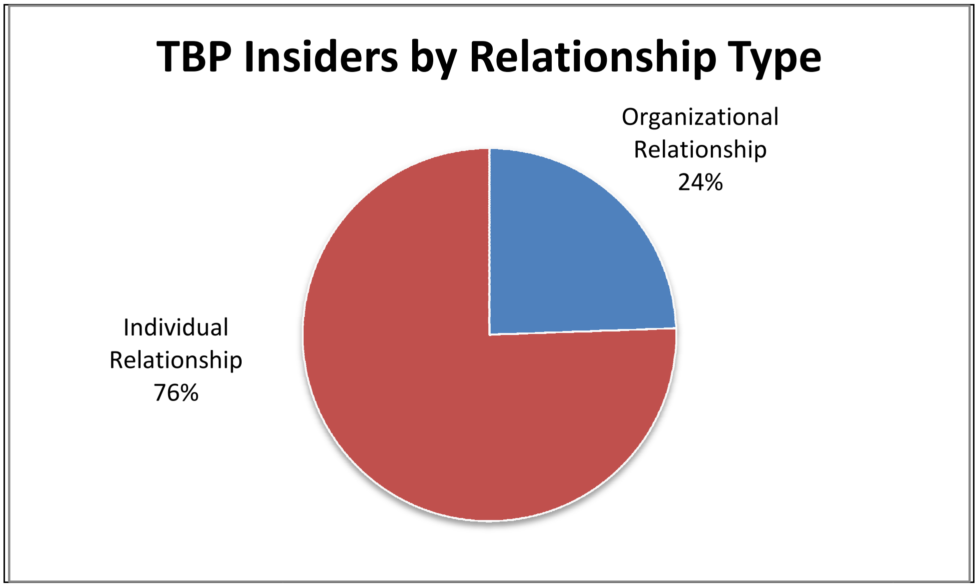

Figure 2 - TBP Insiders by Relationship Type

When an organization forms a relationship with a TBP, its needs may be diverse. For instance, the organization might need employees for either technical or non-technical positions. ***Technical positions*** include any information technology job requires specialized computer skills, such as software developer, network administrator, and IT analyst. ***Non-technical positions*** include any job which does not require specialized computer skills in order to perform a particular job, such as those in data processing, facilities services, or claims processing.

Figure 3 shows the number of cases observed for each type of insider crime classified by employee type: technical or non-technical. The figure clearly shows non-technical TBP insiders were more likely to commit fraud, while technical TBP insiders were more likely to commit IT sabotage.

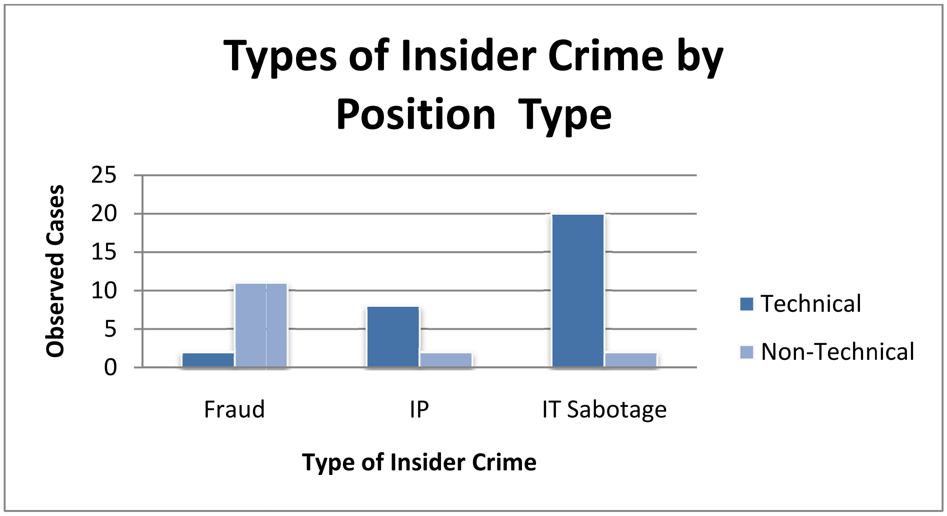

Figure 3 – Types of TBP Insider Crime based on Position Type (Technical/Non-Technical)

Figure 4 presents the number of TBP insiders for each type of relationship (organizational or individual) combined with the type of position held (technical or non-technical). From this analysis, two categories emerge with larger distinct patterns of insider crime. Non-technical insiders in organizational relationships are likely to commit fraud (88%) and technical insiders with individual relationships are likely to commit IT sabotage (74%). In general, across all cases involving TBP insiders, most crimes were committed by males. Age was not a significant factor.

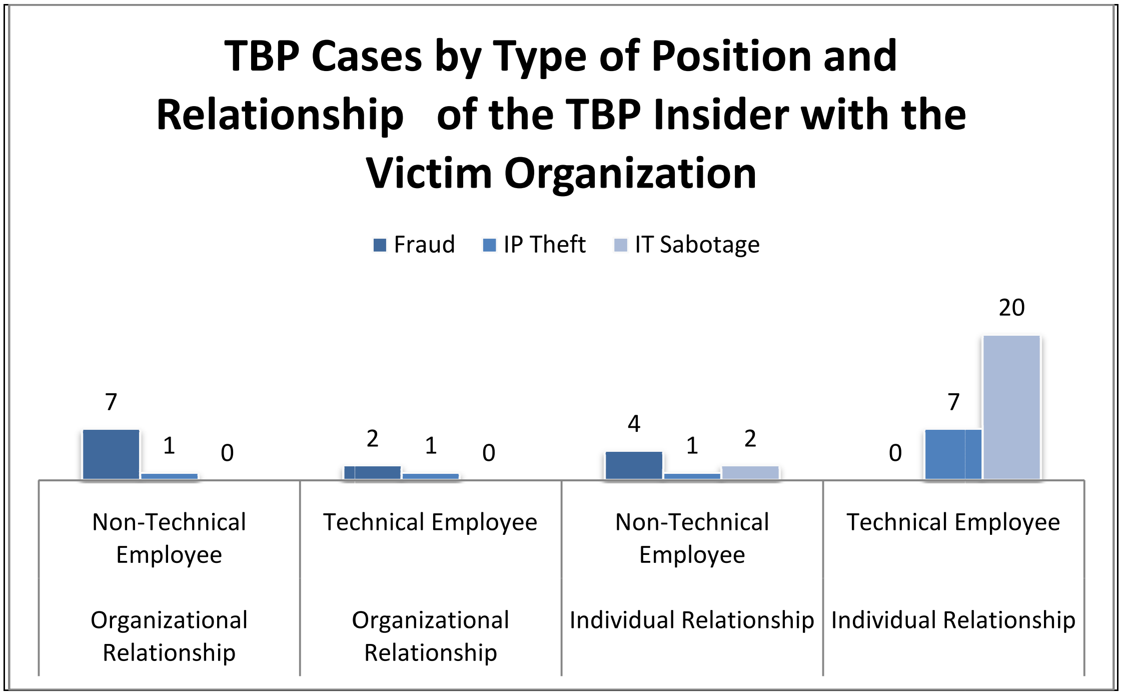

Figure 4 - TBP Cases by Type of Position and Relationship of TBP Insider with the Victim Organization

TBP Insider Case Scenarios and Analyses

Scenario I: TBP Insiders with an Organizational Relationship

The following scenario is based on a typical case of a TBP insider with an organizational relationship with the victim organization. The insider used her access to commit fraud and extort thousands of dollars from the victim organization.

> The insider worked for a trusted business partner that formed a relationship with another organization to handle claims processing. The organization provided the TBP with 10 authorized accounts and a VPN tunnel into its network which could be used from the TBP's remote location. The authorized accounts were able to process claims, add accounts, and modify account details for the organization's clients. The insider processed claims each day for a number of months and became very familiar with the organization's system and its audit controls. The insider realized when claims are expedited no secondary approval is required to settle the claim and mail a disbursement check.

> As a claims processer, the insider did not make a lot of money and she struggled to pay all of her bills on time. She told her boyfriend about the expedited service and he convinced her to expedite a claim in his name to try it out. The insider created a fake claim and a disbursement check was sent to her boyfriend. He cashed the check and they shared the money.
>
> The insider became a bit nervous at work and wondered if anyone knew about what she had done. After a couple of weeks, no one approached her and she assumed it was not likely anyone noticed her actions. Emboldened, she decided to create another expedited claim and another check arrived at her boyfriend's house. The insider and her boyfriend decided suspicions may be aroused if too many claims were filed against one account, so her boyfriend convinced her to expedite and approve claims for his friends. He proposed they split the money with his friends when they cashed the checks.
>
> The insider proceeded to make false claims, and she and her boyfriend were able to recruit a number of friends to help them perpetrate their scheme. Several months later, during a routine audit, a manager at the victim organization noticed an unusually high number of expedited claims were processed using one of the accounts provided to the TBP. The victim organization was able to trace the activity to the TBP insider and shut down the operation. In all, the insider expedited more than sixty false claims with amounts ranging from $100-$1500, costing the company more than $75,000.

Analysis

This was an example of the types of insider crimes that occur with a TBP in an organizational relationship. As noted, organizational relationships arise when an organization outsources a service to a TBP. This case demonstrates what can go wrong when an organization provides a TBP with authorized (but unsupervised) access. In this case, the insider was not technical; she simply observed the claims process.

Examining the cases of TBP insiders in organizational relationships documented in the CERT database, we found all of the observed insiders had authorized access to the systems exploited. All were currently employed at the time of the incident. None of the insiders used remote access from outside the TBP to exploit the victim organization. Over twice as many of these insiders held non-technical positions (8) as held technical positions (3). However, the impact of technical insiders in organizational relationships was much higher. One case involved a help desk employee who created a fake email address to order parts to be sold on EBay costing the victim organization $4.7 million. Overall, for the 5 organizational relationship cases for which we have data, the average loss is $3 million and the median loss is $75,000.

Non-technical insiders are typically assigned tasks that use IT resources to process customer or employee data. Additionally, non-technical insiders tend to be in lower-level positions. In part because of these reasons, non-technical insiders typically exploit the victim organization for financial gain through fraud[2].

Non-technical TBP insiders with an organizational relationship were very likely to commit fraud (88%), while the theft of IP[3] made up the balance of the cases (12%). We did not observe IT sabotage in organizational TBP insider cases. This could be due to the fact that insiders in an organizational relationship usually do not work on site, nor do they have the access privileges necessary to use IT to cause harm to an organization or individual.

Case Summaries: TBP Insiders with Organizational Relationships

The cases summarized below are a sample of cases in which the insider worked for the trusted business partner and had an organizational relationship with the victim organization.

1. The insider was a claims processor at the TBP, which had an organizational relationship with an insurance company. The insider used the authorized access to divert millions of dollars through falsified insurance claims to a personal address. The insider got away with the crime because there was no system in place to double-check the edited claims.
2. The insider colluded with a fellow employee while working as customer support representatives for a TBP that had an organizational relationship with a state government agency. The insiders manipulated state benefit transactions to fraudulently receive $32,000 in food stamp kickbacks and the issuance of food stamps to people who did not qualify. The beneficiaries would pay the insiders with part of the illicit funds they received. The insiders found a flaw which allowed expedited cases to be approved without supervisor authorization. They were caught when the supervisor reviewed records and discovered the illegal activity.
3. The insider worked for a subcontractor to a TBP providing services to a state government agency. The insider used personally identifiable information (PII), credit card information, bank account information, and a state government computer to which she had access to make fraudulent purchases.

[2] ***Insider Fraud*** occurs when an insider uses IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or to otherwise facilitate an *identity crime*. This includes theft and sale of confidential information (for instance social security and credit card numbers), modification of critical data for pay (such as driver's license records, criminal records, and welfare status), and theft of money (from financial institutions, government organizations, etc.). ***Identity crime*** is the misuse of personal or financial identifiers to gain something of value and/or facilitate other criminal activity. See http://www.secretservice.gov/criminal.shtml

[3] The ***theft of intellectual property*** is an insider's use of IT to steal *intellectual property* from the organization. ***Intellectual property (IP)*** is a term referring to original creative thoughts, which includes proprietary information such as patents, copyright material, trademarks, engineering designs and scientific formulas, proprietary source code, and confidential customer information; however, it does not include identity crimes. (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. http://www.cert.org/insider_threat/docs/Insider_Theft_of_IP_Model_MIST09.pdf)

4. The insider was employed as a computer helpdesk agent at a TBP performing computer support for a government organization. The insider created an unauthorized email address and used it to have replacement parts sent to his home. He sold the parts on eBay. The insider made over half a million dollars on the sale of more than 90 parts.
5. The insider was a student who was unofficially working for his uncle. The uncle worked for a document imaging company that was subcontracted by an outside law firm working for the victim organization. The victim organization was a telecommunications company. The insider stole trade secret information and posted it online. When the post was discovered, the FBI investigated the source of the trade secrets posted to the internet and traced the activity back to the student.

Scenario II: TBP Insiders with an Individual Relationship

The following scenario is based on a typical case of a TBP insider with an individual relationship with the victim organization. The insider used his authorized access and privileges to commit IT sabotage against the victim organization.

> An organization just received a resignation notice from its long-time systems administrator. Since it was a small operation, it did not have a second administrator on staff to promote, so it had to quickly hire a contractor to fill the position before the current administrator left the company.
>
> The contractor worked with the outgoing systems administrator for the last month of his employment. The company told the contractor he was being groomed to fill the position and would be hired on full time when his six-month contract ended.
>
> About three months into the contract, the contractor started showing up late. When a manager discussed this with the contractor, he became very disturbed and threatened the manager. After lengthy discussions, the organization decided it should look for someone else to take on the full-time position.
>
> About a month before the contract was set to end, the organization hired a new systems administrator and asked the contractor to train him. The organization informed the contractor he would not be continuing full-time as previously hoped. The contractor became very resentful and set up a fake account with administrative privileges to the network.
>
> That night, he remotely logged into the company using the fake account and planted a logic bomb set to launch malware that could have crippled the company’s network and systems. The logic bomb was set to launch a week after his dismissal. Fortunately, the new administrator discovered the rogue account when reviewing the remote access logs. He also discovered the malicious code before it was implemented and was able to trace the source of the remote login to a specific IP address. Law enforcement traced the IP address to the contractor’s father’s home.

Analysis

This case is an example of a TBP insider in an individual relationship, and it demonstrates how providing privileged authorized access to a contractor can backfire, as well as the risks associated with allowing such individuals to remain on site when they become disgruntled. It also demonstrates how a technical employee could have the knowledge to create backdoor access into a system and plant malicious code capable of causing a great deal of harm to the company.

In the cases of TBP insiders with individual relationships documented in the CERT database, the distinguishing characteristic was the insider's technical role: the majority held technical positions (27) as opposed to non-technical positions (7). Most of these individuals (62%) used an unauthorized means of access to the organizations systems to carry out the attack, e.g., an account that should have been disabled after termination, a backdoor account, or another employee's account. The exploits by technical TBP insiders occurred at the victim organization (53%) or remotely (45%). Of the cases in which the insiders attacked the victim location on site, the overwhelming majority occurred during work hours. Insiders who perpetrated remote exploits of the victim organization typically attacked outside normal business hours.

Technical insiders held positions that provided them with elevated access to the victim organization. Insiders in technical positions typically found vulnerabilities in the victim organization and used their technical knowledge to exploit them.

Revenge was the primary motivating factor in cases involving insiders with individual relationships. It played a significant role in nearly two-thirds of the cases (66%); the objective in these cases was IT sabotage.[4] These individual TBP insiders sought revenge for not being offered full-time employment with the victim organization, for not having their contract renewed, for not receiving a positive performance review, or for other grievances.

In the other third of cases, the insider was motivated by financial gain (17%) or competitive business advantage (17%). This explains why this subset of insiders targeted the intellectual property of the victim organization.

[4] Note that this crime fits the pattern of the typical insider IT sabotage attack, regardless of whether the insider is an employee or a TBP. ***Insider IT sabotage*** is an insider's use of IT to direct specific harm at an organization or an individual. Examples include the malicious deletion of organizational information, bringing down organizational systems, and web site defacement to embarrass the organization. (Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. "The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures" in Insider Attack and Cyber Security: Beyond the Hacker, eds. Stolfo, S.J., et. al., Springer Science + Business Media, LLC, 2008. Also published as an SEI Technical Report - CMU/SEI-2008-TR-009. http://www.cert.org/archive/pdf/08tr009.pdf)

Case Summaries: TBP Insiders with an Individual Relationship

The cases summarized below are a sample involving insiders from a TBP who had an individual relationship with the victim organization.

1. The insider had been contracted through the TBP to work on the IT staff of a telecommunications company, but was terminated for poor performance. After his termination, he used his company-issued laptop to access the victim organization's network and use a shared password, which had not been changed since his departure, to access user accounts. The insider was caught when an employee at the victim organization noticed her last login was time stamped only a few hours previous, a time at which she was not logged into the system. This led to an investigation of the logs, which discovered the insider's actions.
2. The insider was a software development consultant for an IT company. The insider wanted a share of the company, which he demanded over the course of a year. The victim organization refused the insider and gave him a three-month notice of the termination of his contract. The insider logged into the system, deleted files, and blocked access to the company's system until his demand was met. The company reported the insider to the FBI, who arrested the insider.
3. The insider was hired through the TBP as a temporary helpdesk agent and network technician in the customer support department of an IT company. The insider wanted to be hired as a full-time employee, but was informed he would be terminated. As a result, the insider wrote several threatening emails, which led to his immediate termination. In retaliation, the insider used his remote access channels to access the victim organization's network, change administrative passwords, remove network access to systems, delete event logs, and modify the accounts of people involved with his termination.
4. The insider was a systems administrator for a TBP that was a contractor to a government agency. The insider's supervisor reprimanded him for frequent tardiness, absence, and unavailability for work. The insider planted a logic bomb on the government organization's server to delete critical files. The insider attempted to conceal his activities by removing history files, creating malicious code to overwrite itself after execution, and framing his supervisor for the malicious act. The insider was caught after arousing suspicion by constantly calling the victim organization to check on the system servers after his termination. Fortunately, the logic bomb never executed.
5. The insider was employed by the TBP as a contract engineer for a manufacturing company. Angry at his supervisor and in fear of losing his job, he disclosed technical drawings to the competitor of the victim organization.

Summary Observations

Table 1 displays the statistics of observed cases for TBP insiders categorized by organizational relationships and individual relationships. As explained in this article, there are significant differences in the risks exploited based on this relationship.

Table 1 - Statistics of TBP Insiders Based on Relationship with the Victim Organization

	Organizational	Individual
Type of Position		
Technical	**27%**	**79%**
Non-Technical	**73%**	**21%**
Authorized Access		
Authorized Access	**100%**	**38%**
Unauthorized Access	**0%**	**62%**
Location		
At Trusted Business Partner	**82%**	**53%**
At Victim Organization	**0%**	**3%**
Either TBP or VO	**18%**	**0%**
Remote Access	**0%**	**44%**
Type of Insider Crime		
Fraud	**82%**	**12%**
Theft of Intellectual Property	**18%**	**24%**
Sabotage	**0%**	**65%**
Motive for Insider Crime		
Financial Gain	**73%**	**12%**
Revenge	**0%**	**53%**
Business Advantage	**8%**	**18%**
Prestige	**8%**	**3%**
Unknown	**8%**	**15%**

In summary, TBP insiders in an organizational relationship held mostly non-technical positions, while TBP insiders with an individual relationship held more technical positions. In order to commit the insider crime, TBP insiders in organizational relationships used their authorized access, whereas TBP insiders in individual relationships used unauthorized access to commit the insider crime. This difference likely affected the location from which the insider committed the crime. The TBP insiders in organizational relationships only used access from the TBP site or the victim organization. The TBP insiders in individual relationships used remote access paths for their exploits. Finally, insiders with the organizational relationship were more likely to commit fraud motivated by financial gain. The TBP insider in an individual relationship was often seeking revenge and committed sabotage in retaliation.

Recommendations for Mitigation and Detection[5]

This section summarizes a set of recommendations for organizations concerned about malicious acts by employees of trusted business partners.

[5] Cappelli, D. M., Moore, A. P., Shimeall, T. J., & Trzeciak, R. J. *Common Sense Guide to Prevention and Detection of Insider Threats: 3rd Edition*. Report of Carnegie Mellon University, CyLab, and the Internet Security Alliance, September 2008 (update of earlier editions).

Recommendation 1: *Understand the policies and procedures of the trusted business partner.* An organization establishes policies and procedures in order to protect their own goals. However, when an organization considers enlisting the support of a trusted business partner, they should ensure that the TBP's policies and procedures are at least as effective as their own safeguards. This includes physical security, staff education, personnel background checks, security procedures, termination, and other safeguards.

Recommendation 2: *Monitor intellectual property to which access is provided.* When organizations establish an agreement with a trusted business partner, they also need assurance the intellectual property they provide access to is protected. Organizations need to get assurances that access to and distribution of this data is monitored. Organizations should verify there are mechanisms for logging the dissemination of data. Organizations should be aware of procedures that the trusted business partner has to investigate possible disclosure of their information.

Recommendation 3: *Maintain access rights management.* When contracting with a trusted business partner to handle sensitive data, it is important for the organization to know how data is going to be managed. In a number of cases, the trusted business partner could not handle the full work load it took on and subcontracted to another organization or brought in temporary employees in order to be able to process the job. The organization should be aware of these arrangements and ensure the data will be handled by means acceptable to the organization.

Recommendation 4: *Understand the personnel policies and procedures of the trusted business partner.* When contracting with a trusted business partner, the organization should insist that the partner organization's employees are investigated and cleared to handle data in ways similar to their own employees. In a few cases, the trusted business partner employed workers with criminal backgrounds or connections to the Internet underground. Organizations should not compromise the level of security in order to have a job accomplished faster.

Recommendation 5: *Anticipate and manage negative workplace issues.* When an organization decides to hire consultants, contractors, or temporary employees they should be made aware of the organization policies and practices for acceptable work behavior. Negative workplace issues have been known to trigger illicit insider activity; it is important that policies and procedures for managing such events consider permanent employees, contractors, consultants, and temporary employees. It is also important that organizations do not provide false hope for these employees regarding likelihood of being hired. If a company has indicated they may hire a contractor or consultant full time but then decides not to do so, they should perform an assessment of the individual's insider risk. They should remove the individual's access and change any shared accounts that access was provided in order to mitigate risks when the individual is informed he/she will not be hired. It has proven risky to retain the services of disappointed or disgruntled temporary workers.

Recommendation 6: *Deactivate access following termination.* When an employee, consultant, or contractor is terminated or suspended, all access that the person had should be disabled. When organizations are forming an agreement with a trusted business partner, they should make certain the trusted business partner performs rigorous termination procedures as well. In a number of cases involving contractors, access was not disabled immediately after termination and the insider was able to exploit that access in the commission of their crime.

Recommendation 7: *Enforce separation of duties.* A number of insiders exploited the fact that certain actions could be performed in such a way that circumvented normal separation of duties controls. Business processes should enforce separation of duties, regardless of the speed or priority required. While different levels of controls may be associated with different priority tasks, no processes should be left without protections against possible exploitation by a disgruntled or greedy insider.

Recommendation 8: *Create clear contractual agreements that make it clear the TBP is also responsible for protecting organizational resources.* Contracts with a trusted business partner should include restrictions on how the TBP handles and shares the information. This should include restrictions on the TBP's ability to subcontract with other organizations on tasks involving sensitive information. There should be standard terms and conditions that allow the organization to apply the same policies and procedures to contractors, subcontracts, and consultants that it applies to its own employees including mandatory flow-down provisions from prime contractors to subcontractors. Also, contracts should include notification requirements for breaches and termination of key employees. The contracting organization should make its security requirements clear and also develop consequences which will incentivize the TBP to protect key resources.

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).