Software Engineering Institute

Spotlight On: Malicious Insiders and Organized Crime Activity

Chris King

January 2012

TECHNICAL NOTE
CMU/SEI-2012-TN-001

CERT® Insider Threat Center

http://www.sei.cmu.edu

Carnegie Mellon

This material is based upon work funded and supported 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 sponsored by the United States Department of Defense.

This report was prepared for the

SEI Administrative Agent
ESC/CAA
20 Schilling Circle, Building 1305, 3rd Floor
Hanscom AFB, MA 01731-2125

Table of Contents

List of Figures

Abstract

This report is based on the fifth article in the Spotlight On quarterly series published by the CERT® Insider Threat Center. 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. The focus of this report is on current or former employees, contractors, or business partners who were affiliated with, or are considered to be part of, organized crime. The case material came from a mixture of court documents, Department of Justice press releases, interviews, and media reports. This report defines malicious insiders and organized crime and provides a snapshot of who malicious insiders are, what and how they strike, and why. This report concludes with a summary of the relevant details of the highlighted cases and offers recommendations that could potentially mitigate the risk of similar occurrences.

1 What Is Organized Crime?

The Federal Bureau of Investigation (FBI) defines organized crime as

> *"Any group having some manner of a formalized structure and whose primary objective is to obtain money through illegal activities. Such groups maintain their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion, and generally have a significant impact on the people in their locales, region, or the country as a whole"[FBI 2011].*

Criminal enterprises mask their fraud by involving multiple insiders who often work in different areas of the organization and who know how to bypass critical processes and remain undetected. In several cases, management is involved in the fraud. Those insiders affiliated with organized crime are either selling information to these groups for further exploitation or are directly employed by them.

2 Organized Crime and Malicious Insiders

Ties to organized crime appear in only 24 cases[1] in the CERT® insider threat database and are characterized by multiple insiders and/or outsiders committing long-term fraud.[2] All of the insiders involved with organized crime attacked the organization for financial gain. The insiders usually were employed in lower level positions in the organization, were motivated by financial gain, and were recruited by outsiders to commit their crimes. The average damages in these cases exceed $3M, with some cases resulting in $50M in losses.

This report discusses the two different types of insider organized crime activity:

- insiders with ties to existing external organized crime groups
- insiders who form or participate in their own criminal enterprises. A criminal enterprise is a group of six or more individuals with an identified hierarchy, or comparable structure, who engage in significant criminal activity [FBI 2011].

Here is a sample case involving a criminal enterprise:

> Five insiders worked for a credit reporting company. Each of them was a low-level employee with job responsibilities of data entry and modification of credit reports. A car salesman befriended one of the insiders while the insider was shopping for a car and found out what the insider's job entailed. He offered to pay the insider $150 per record to change credit reports of individuals who wished to purchase a car but had insufficient credit. The insider then recruited his colleagues to participate in the scheme. Each week the outsider dropped off the names of the individuals and associated payments. The organization had a business process in place to verify changes to credit reports, but two of the employees involved in the scheme had the authority to override the verification process. The fraud continued for over a year until a routine audit discovered the discrepancy.

Here is a sample case of external organized crime:

> An insider worked for a large U.S. bank as a teller. He handled customer information on a daily basis and processed checks for customers. Heavily in debt, the insider was approached by individuals in the mafia who offered to pay him to steal customers' personally identifiable information (PII). Over the course of several years, the insider sold PII to the organized crime group, that in turn used it to create fraudulent checks, open unauthorized credit cards, and commit identity theft. The theft was caught when the bank became suspicious of the exceptionally high rate of fraud occurring in one of its local branches.

[1] See Appendix A for detailed information on these cases.

[3] CERT conducted interviews for approximately 150 cases; interviews included victim organizations, prosecutors, investigators, and 3 convicted insiders.

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

2.1 Who They Are

This report is based on 24 cases that involved a criminal enterprise (20 of the cases) or external organized crime (4 of the cases). The majority (14) of the insiders in these cases were employed in nontechnical positions, and four held management positions. The crimes involving management went on for longer periods of time, and the scale of the crimes was much larger. The majority of the insiders were female (16), which is greater than the standard profile of all fraud cases in the CERT database (roughly 50 percent male/female). Finally, there was a large amount of outsider collusion (21 of the cases). Each criminal enterprise had six or more conspirators, usually with a number of outsiders who were either the leader or assisted with the crime. In cases involving existing organized crime groups, fewer insiders tended to be involved.

In the crimes involving management, the average loss was very high. One case involving a manager at a Department of Motor Vehicles (DMV) caused losses of $250,000; another DMV case resulted in a $1M loss for the organization. The most damaging case involved an insider working for a city tax office, who was able to steal $48M over the course of almost two decades. These insiders were low- or mid-level management with few technical skills. They used their deep knowledge of the organization's processes and systems to bypass the checks and balances in place and recruited their subordinates into the crime.

2.2 Why They Strike

Insiders held low-level positions in the organization and committed the crimes for financial gain. As such, all of the incidents in this subset of cases were done for financial gain.

2.3 What They Strike

Insiders primarily copied or modified data. Crimes included stealing customer information to sell for identity theft, modifying credit reports to give buyers a higher credit score, or creating fake credentials, such as driver's licenses. Insiders primarily modified data in organization databases and bypassed integrity checks.

2.4 How They Strike

Seventy-one percent of the attacks occurred on-site during normal working hours. For the most part, insiders used their authorized access to copy, modify, or delete critical data from the organization's systems.

The technical methods used included:

- social engineering to obtain credentials or information

  An insider, after resigning from a law enforcement agency, convinced colleagues to run searches and gather information on companies to help him and his conspirators perform insider trading.

- authorized use of an organizations' systems

  An insider used his access to customer credit reports to sell the data to conspirators who would conduct identity theft.

- bypassed secure processes

  An organization required two employees to issue tax refund checks, but both insiders in the process were part of the same criminal enterprise and would issue fraudulent checks to their conspirators.

- compromised accounts

  An insider working for a credit-reporting agency performed modifications of customer credit in exchange for money. The insider used stolen passwords of coworkers to conceal evidence of the crime.

3 Organizational Issues of Concern and Potential Countermeasures

Each incident in our database is tagged with issues that we see recurring throughout all the cases. This tagging allows for the identification of particular trends that are associated with different types of cases. The following graph depicts organizational issues of concern in these cases.

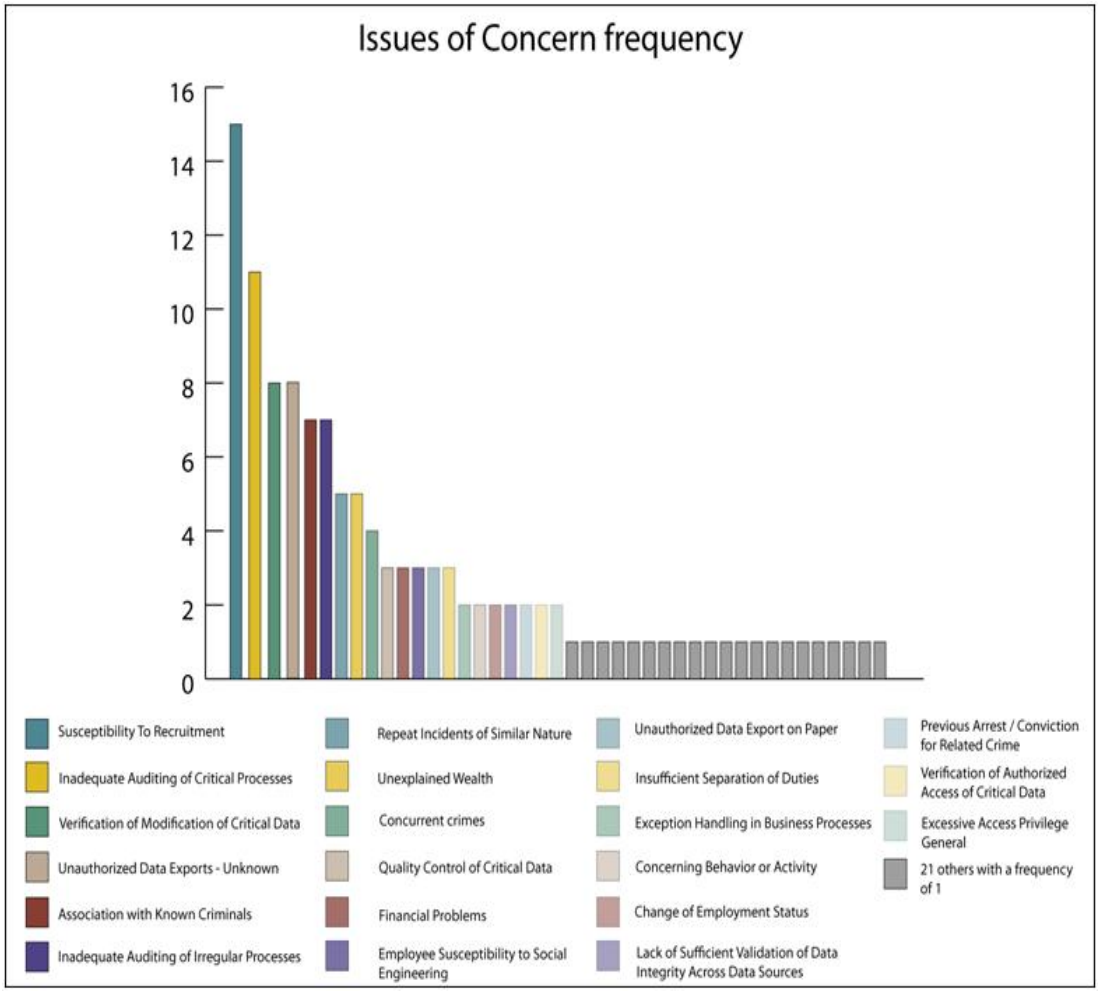

Figure 1: Issues of Concern Frequency

Suggestions for identifying and mitigating the most common issues of concern from the graph above are discussed in the sections that follow. The issues *of inadequate auditing of critical processes* and *inadequate auditing of irregular processes* have been combined due to their similarities. The issue of *unauthorized data exports – unknown* will not be discussed, since it represents a lack of data for that particular case.

3.1 Employee / Coworker Susceptibility to Recruitment

Fourteen of the cases involved outsiders from organized crime who approached employees of the victim organizations and offered to pay them in exchange for some service, often the unauthorized modification of data.

The following incidents are examples of how an outsider from organized crime was successfully able to recruit an insider to commit a crime.

1. The insider worked at an insurance company and began stealing PII that included customers' banking information. The insider then sold this information to an outsider co-conspirator who created fraudulent checks for various banks using the customers' PII. The insider and outsider then had "check-runners" cash the checks at various banks, posing as legitimate customers, thus making fraudulent withdrawals from their accounts. The insider also passed on the customers' information to individuals who created fake identification (IDs) and counterfeit checks in the customers' names. Multiple employees from several different banks were recruited for this scheme.
2. The insider was employed as a service representative for the victim organization. After several years in her current position, the insider was approached by a Nigerian male with ties to the Nigerian mafia. The insider, facing financial difficulties, agreed to provide the man with personal information from victim organization's Social Security Number (SSN) records at a rate of $15-$20 per SSN record. A few months later, several major financial institutions reported fraudulently issued and authenticated cards. The subsequent investigation led back to the insider, who confessed to law enforcement, resigned from her job, and was subsequently arraigned and pled guilty. The insider was sentenced to 10 months in jail, 2 years of probation, and was ordered to pay $10,000 in restitution. The impact of this scheme is unknown, but several financial institutions had to reissue credit cards and implement fraud monitoring on customer accounts.

Both of these cases involved outside recruitment, which can be hard for an organization to detect, especially if it occurs during off hours. Organizations should train managers and employees to recognize and report suspicious contact in which an insider approaches other employees to join in their crime. Having employees who understand the potential for insider recruitment and the consequences of committing such an act may decrease the risk of recruitment and increase reporting.

Training should be based on organizational policy and include a confidential process for reporting security issues. Confidential reporting allows reporting of suspicious events without fear of repercussions. Employees should understand that the organization has policies and procedures and be aware that managers will respond to security issues in a fair and prompt manner [Cappelli 2009].

3.2 Inadequate Auditing of Critical and Irregular Processes

In 10 cases, insiders remained undetected for long periods due to inadequate auditing of critical or infrequent business processes. In one incident, malicious insiders were able to modify records at the DMV because there was no auditing in place. In a second incident, an insider was able to submit false credit reports to the credit bureaus by social engineering her management into exempting her department's activities from the auditing process. Details of these cases follow.

1. A licensing and registration examiner at a DMV conspired with nine other accomplices to sell fraudulent IDs and driver's licenses. A sample fraudulent license or ID would have a customer's real record with a picture of the criminal enterprise's client. Besides the insider, the criminal enterprise had four DMV employees (with smaller roles in the case) and five outsiders (three brokers and two recruiters). Most of its clients were illegal immigrants desperate for driver's licenses or identity cards. The insiders were employees who had authorized access and occupied low-level positions in the organization. The DMV's computer system was designed to cross-check SSNs with the Social Security Administration, but the employees found a way to bypass that check. The insider either used bogus SSNs or stole actual SSNs from the DMV system without being flagged by security. The ring made $800,000 in illicit profits from selling the fraudulent credentials.
2. The insider worked for a tax office preparing property tax refund checks. The insider generated tax refund checks to bogus companies, then gave the checks to her niece. Her niece deposited the checks into the bank accounts of the fake companies and then distributed the funds to various members of the scheme. Since the insider played a role in designing her organization's new computer system, she convinced management that her department should not be included in the auditing process. The insider's malicious activities were then processed outside of the new auditing system. The insider was able to steal $48M over the course of almost 20 years.

Both of these cases involved nontechnical overrides of critical processes. Vulnerabilities in critical processes should be included in an organization's risk assessment to properly identify, track, and respond to vulnerabilities in business processes. Periodic audits of the work products from these types of critical processes should be conducted to detect abuses of the system.

3.3 Association with Known Criminals

Four cases involved affiliation with organized crime groups. These insiders either came into the victim organization already part of such a group or were recruited later on. Details of two of the cases follow.

1. The insider was part of an organized crime family and used his access to a law enforcement intelligence database to steal PII. The PII was used to commit identity theft, check fraud, and other racketeering activities. The insider was paid in gifts, drugs, and cash for his services to the crime family. The crime family also used the information provided by the insider to scout for potential extortion targets and increase the reach of its organization. The impact was in excess of $2M dollars.
2. The insider was part of an elaborate organized crime ring that used names of medical providers to submit false Medicaid claims. The leader, an outsider, used the insider (who worked for an IT contractor for a medical billing company) to get the names of medical providers who rarely filed claims and send in change of address forms. The payments were redirected to a post office box, where the group would pick up the checks and cash them using a check-cashing business that did not verify identification. The group was successful in laundering over $1.5M in false claims over four years.

These two cases are examples of employees with ties to criminal organizations. The first step in preventing this issue of concern is to perform background checks on individuals before hiring

them. Background checks should investigate previous criminal convictions, include a credit check, verify credentials and past employment, and include discussions with prior employers regarding the individual's competence and approach to dealing with workplace issues. This information should be used as part of a risk-based decision process in determining whether it is appropriate to give the new employee access to critical, confidential, or proprietary information or systems.

Background checks should be required for all potential employees, including contractors and subcontractors. In one recent case, an organization employed a contractor to perform system administration duties. The hiring organization was told by the contractor's company that a background check had been performed on him. The contractor later compromised the organization's systems and obtained confidential data on millions of its customers. The investigation revealed that the contractor had a criminal history for illegally accessing protected computers.

Providing current employees with training and a process for reporting suspicious contacts or activity may reduce this threat.

3.4 Verification of Changes to Critical Data

In six cases, insiders were able to carry out their crime because the organization did not review critical data when it was modified. Insiders used authorized access and were able to change data without oversight. Details of two sample cases follow.

1. The insider worked at a consumer credit-reporting agency and maintained information stored in the consumer credit database. In exchange for money from outsiders, the insider conspired with other employees to artificially inflate the credit scores of consumers to enable them to secure loans from third-party credit institutions and lenders. She and her insider conspirators modified or deleted 178 consumers' credit-history data contained in the database. The purpose was to strengthen their creditworthiness, and the impact was that lenders issued $4.2M in new loans to these consumers. The insider admitted that her actions caused lenders to detrimentally rely on false credit reports and to extend new loans to those consumers. She passed on payment from consumers to her conspirators and received payment from her external conspirators.
2. Over six months, two case workers from a firm distributing child-care vouchers manipulated state computers to illegally pay benefits to people who did not qualify. The insiders manipulated the food stamp distribution system by opening food stamp cases or increasing monthly allotments on existing cases. They were able to carry out their crime by exploiting a weakness in the system's exception handling: if the food stamp request was coded as an expedited case, the caseworker could open it without a supervisor's authorization. The caseworker could open food stamp cases even when recipients did not provide personal information. For payment, each recipient turned over a portion of the monthly food stamp allotment, resulting in the case workers pocketing $32,000 in food stamp kickbacks.

Frequent, random audits of system databases should verify the information entered since the last audit. Additionally, automated flagging of mismatched data may detect improper modifications of the databases. External audits of these databases can also uncover fraud that may be concealed by an internal audit.

4 Conclusions

Insiders that lead or join an organized crime group can be more difficult to detect than a lone insider in an organization. A motivated group of insiders can bypass normal checks and balances by reaching across departmental boundaries—often with management complicit in the crime. Insiders affiliated with external organized crime groups have the resources of a large organization available to help them in their crime. This can include multiple insiders working for several organizations that are all part of the same criminal group. The impact of insiders and organized crime exceeds a normal fraud case and can cause $3M in damages on average, and up to $50M in the most extreme case.

To combat this type of insider threat, organizations should follow these recommendations:

- **Conduct detailed background investigations of individuals they want to employ.** Some of the insiders affiliated with organized crime had these contacts before they were hired. Other insiders had high amounts of debt or other personal issues that made them susceptible to recruitment, by malicious outisiders.
- **Audit all critical and irregular processes on a frequent basis.** Insiders exploited the lack of auditing or poor auditing to conduct their crimes.
- **Audit modifications to critical data on a frequent basis.** Insiders with authorized access can make unauthorized modifications to critical databases without detection. Frequent auditing of changes to critical information can identify unauthorized changes.
- **Conduct external audits of processes and systems.** Insiders involved with organized crime and criminal enterprises often had multiple insiders involved in the crime. External audits can identify discrepancies and eliminate collusion.

Appendix A: Cases from the CERT Insider Threat Database That Involve Organized Crime

Case #	Total Conspirators	# Insiders	# Outsiders	Impact	Insider Led?
1	10	4	6	$48,115,451	Yes
2	94	1	93	$10,000,000	No
3	4	3	1	$6,775,434	Yes
4	3	1	2	$2,700,000	Yes
5	14	13	1	$2,288,946	Unknown
6	10	1	9	$1,500,000	Unknown
7	7	2	5	$1,000,000	No
8	4	1	3	$841,164	Yes
9	10	5	5	$800,000	Yes
10	6	1	5	$638,000	No
11	6	2	4	$335,000	No
12	16	6	10	$287,500	Unknown
13	4	4	0	$250,000	Yes
14	6	1	5	$231,500	Yes
15	6	1	5	$157,000	Unknown
16	16	1	15	$77,300	No
17	6	2	4	$75,000	Yes
18	2	1	1	$10,000	No
19	8	2	6	Unknown	No
20	4	2	2	Unknown	No
21	9	5	4	Unknown	Yes
22	11	1	10	Unknown	No
23	Unknown	1	Unknown	Unknown	No
24	21	1	20	Unknown	Unknown

References

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

[Cappelli 2009]

Cappelli, Dawn, Moore, Andrew, Trzeciak Randall, & Shimeall, Timothy. *Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1*. Software Engineering Institute, Carnegie Mellon University, 2009. http://www.cert.org/archive/pdf/CSG-V3.pdf

[FBI 2011]

The Federal Bureau of Investigation. *Glossary of Terms.* http://www.fbi.gov/about-us/investigate/organizedcrime/glossary (2011).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2012	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Spotlight On: Malicious Insiders and Organized Crime Activity	FA8721-05-C-0003

6. AUTHOR(S)

Chris King

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2012-TN-001

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
ESC/CAA 20 Schilling Circle, Building 1305, 3rd Floor Hanscom AFB, MA 01731-2125	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report is based on the fifth article in the Spotlight On quarterly series published by the CERT® Insider Threat Center. 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. The focus of this report is on current or former employees, contractors, or business partners who were affiliated with, or are considered to be part of, organized crime. The case material came from a mixture of court documents, Department of Justice press releases, interviews, and media reports. This report defines malicious insiders and organized crime and provides a snapshot of who malicious insiders are, what and how they strike, and why. This report concludes with a summary of the relevant details of the highlighted cases and offers recommendations that could potentially mitigate the risk of similar occurrences.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Insider threat, malicious insider, organized crime	20

16. PRICE CODE

20117 74 1160455 | THREAT & INCIDENT MGMT*Threat & Inc Mgmt Li *5-001A SEI-LINEC05

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