Southwestern College

Investigation in the Workplace

Security Investigation

Portfolio Assignment

Computer Crimes Investigation

Identity Theft

By

Samuel L Alva

**Introduction**

I will be discussing a case involving a military member who was charged with identity theft. I will discuss his military career and what lead Tom Doe into stealing critical information which he then used to open credit cards and purchase items all over the United States. I will discuss how he was able to evade authorities for years before getting caught red handed. I will discuss methods used to conduct the investigation to include physical security, electronic surveillance, undercover work and search warrants each having providing their own crucial element.

**The Basis of the Investigation**

This case involved a military individual by the name of Tom Doe, he is maintenance troop with the 22nd MXS squadron out of McConnell AFB, Kansas. He joined the military right out of high school is married and has three kids. Tom Doe is an E-6 and besides doing his normal job as a maintenance troop he has extra duties. One of his extra duties is being a security manager, as a security manager it’s your job to make sure individuals within your unit are following rules and regulations concerning information and computer use. Also as a security manager it’s your job to make sure security clearances are processed when they need to be. Information that goes into a security clearance is very detailed, besides having your social security number on every page there is other information like where you have lived for the last ten years and every other piece of information that can easily be used against you to steal your identity. Tom Doe has been stationed at McConnell AFB for about 10 years; he knows the system in and out and was comfortable where he was.

Tom Doe lived lavish life with his family, his wife of 5 years who is a registered nurse. When the investigation begins, Mr. Doe was being investigated for financial identity theft and grand Larceny. Though he was caught with evidence in hand investigators weren’t quite sure how he was able to get away with it for so long and how did he choose his victims.

OSI (Office of Special Investigation) agents investigate cases for the United States Air Force. OSI agents are responsible all investigation other than minimum drug use and minor crimes. This case was brought to our attention for a couple of reasons. The victims associated with this investigation had been stationed together at this installation and are now stationed together at their current installation. Both cases had their identities stolen roughly at the same time. Both individuals worked in the same unit but did not know one another at the time. To give some background to how the Air Force works, it is made up of different wings, squadrons and units, each providing a service that is vital to national security and the safety of the United States. These individuals worked in maintenance squadron fixing and maintaining KC-135’s. KC-135’s are the gas stations in the sky providing JP-8 to multiple fix wing aircraft in the DOD arsenal.

Recently personal at McConnell AFB have seen a spike in identity theft cases, since most cases have gone undetected due to lack of security policies that currently exist, some damages were higher than others. Since this issue initially had no bearing with the military most of the victims some even geographically separated suspected any foul play from the military. Since those affected didn’t suspect foul play they assumed someone got ahold of their information. As several months passed individuals who required a Top Secret clearance to conduct their job were affected. When obtaining a Top Secret clearance your entire life is investigated. One of the primary questions asked “Have you been late on any payments for 90 days or longer”?, when individuals identities are stolen, criminals will immediately open up as many credit card accounts as possible as well as charge them up quickly.

**The Objectives of your investigation**

Before conducting the investigation you must set your objectives for a couple of reasons. Experience has shown that carefully crafting the objectives provides substantial dividends later on in the investigation if you are ever challenged on your process. (Ferraro, 2012) Identifying you objectives is crucial, it allows you to articulate what you are trying to get of of the case.

* **Seek out and identify the true nature and scope of the problem**: Identifying the nature and scoop of the problem is essential in making sure you don’t get side track by loose ends. In this case Mr. Doe is accused of stealing critcal information and utilzing it maliciously.
* **Identify who is involved and why.** Identifying who is involved is very important due to possible accomplices, the nature of the crime and the amount that was stolen, the suspect could have had an accomplice.
* **Gather any and all information in such a fashion as to allow the proper distribution of disciplinary and/or corrective action when appropriate**. Being able to gather the right evidence is crucial in giving those who are going to be reviewing it the right tools to excute the correct punishment.
* **Engineer the process in such a fashion that is least disruptive to the organzaiton and its operation.** When conducting the investigation you must make sure that your investigation doesn’t disrupt normal operations. Mr. Doe is currently in confinement and will remain their untill the case is brought to court and he is proven innocent or guilty.
* **Achieve the best possible return on investment.** Achieving the best possible return on investment is really not an priority on this case, the victims affected by this case had their lives disrupted and credit disrupted.

**The logical Application of each of the six methods**

**Physical Surveillance:** will be used to identify items purchased by suspect or any other physical evidence that may bring light to the case. Physical surveillance involves people watching people, places or things. (Ferraro, 2012) Stationary and moving surviellance which allows the investigator the ability to move from one location to another, which will help since the suspect has been opening credit cards in multiple states. Since some of the crime were committed in multiple state juridication may be an issue. The project manager being an OSI agent and working for the Department of Defense has the autherity over anyone under the USMJ (The Uniform Code of Military Justice). The Uniform Code of Military Justice (UCMJ) is a federal law, enacted by Congress. Its provisions are contained in United States Code, Title 10, Chapter 47. Article 36 of the UCMJ allows the President to prescribe rules and procedures to implement the provisions of the UCMJ. The President does this via the Manual for Courts-Martial (MCM) which is an executive order that contains detailed instructions for implementing military law for the United States Armed Forces. (Powers, 2012) Since the individual is an Active duty member of the United States Military any crimes committed in any state or country doesn’t require any special type of jurisdication. OSI agents are equivelent to FBI agents, so when there isnt an Air Force Base installation near they can contact a FBI field office and get assistance. Video imaging technology has come along way, depending on the type of evidence required video imaging has gotten pretty advanced. Before running countless wires all over your facility and bluilding for analog CCTV (Closed Circuit Television)was normal when incorperating video feeds for a command post of covert videoing. Now we have wireless and IP cameras which can be ecrytpted and signals can be sent anywhere in the world. Which if set up correctly surviellance can be accomplished any where in the United States or the world.

**Electronic surviellance**: will be used tremendous, electronic surviellance involves any type of surviellance involving electronic access control technology, computer use and monitoring, alarm using electronic warning and monitoring technology. Since most of the crimes were committed using a computer to open credit cards and purchases items online, computer monitoring will be a tool used greatly. Computer monitoring has come along way, depending on the search warrant certain computers can be monitored continueasly or live depending on the type of information being searched for.

**Research and Audit** will be used to analyze informaton from multiple sources both internally and externally. Since OSI was able to get jurisdction they were able to review not only Mr. Doe’s personal finacial records but the victims as well. Hundreds of records were reviewed indentifying hundreds of personal who could have had their identity stolen. There was no rhime or reason who Mr. Doe choose to steal there identity but since the security manager were on the list of individuals who yoo need to see when you out process, gave the Mr. Doe a selection process. He did however choose individuals who had good credit making sure when he applied for credit it would go through.

**Forensic Analysis:** will be prodomenently due to the crimes committed being on a computer. Computers confiscated may have to be analyzed for information containing unautherized information of the victims. This will require a computer forensic to analyze the information he may have stoled to steal critical informaton allowing him to open up credit cards in someon elses name.

**Undercover:** work may be an option to catch said suspect in the act, there were reports that said suspect used stolen credit cards at local resturants. If under cover opertions were to be conducted it would be to catch the individual in the act of using stolen credit cards.

**Interview and Interrogation:** Interviews will be conducted due to multiple victims and witnesses. Since most of the witnesses and victims are geographically seperated made it difficult and time cosuming when gathering testomonies.

**Search Warrents:** will be issued to not only look through credit reports but to search the suspects home and belongings. Since the amount stolen was over 100,000 the individual will be charged not only with finacial identity theft but grand larceny.

**A grand:** A jury of his peers will be assigned to decide his fate in court. Since he is in the military a jury of his peers will be choosen from military members both officers and airmen will be choosen to review and decide if he is guilty of the crimes committed.

**Project management and Case Development**

Once all your information is in order it is time to build your team. The investigative team will consist of your fact finders, in this case other OSI agents, security policemen and Department of Justice personal. In this case the OSI agent will be the project manager, he will make sure that the case follows a specific path and make sure the investigation stays on course. The proposal is simple; gather the right information either to prove his innocence or his guiltiness. Your Fact finders are going to be your key in making sure the information is collected in an ethical and efficient manner. Mr. Doe was told initially that if he cooperated his sentence would be taken in consideration. The fact finders were able to reveal that Mr. Doe was using his position as a security manager to gather all the information he needed to create/open credit cards. Once he opened them he initially never made purchase in the local area. When making purchases they were made out of state on his home computer mostly where Mr. Doe had family members. Since the members whose information was stolen never associated their crimes with the military they never thought to accuse the Air Force of foul play. After interviewing witnesses located here and victims stationed at other location, we were able to discover two things. Witnesses here that were friends or co-workers indicated that Mr. Doe lived a very lavish life style even wondering how he was able to afford items he had like new cars, big screen TV’s and furniture that didn’t fit with his pay scale. Two, two of the individuals accidently met at the legal office at their current base, they were there for the same reason, and both of their identities were stolen. As they were discussing the similar issues, they figured out that they were stationed at the same base previous to the one they are at currently. After reviewing where some of the charges were made, they also came to the conclusion that some of the charges were from the same place. They contacted OSI at their current location and the investigation started.

Back at McConnell AFB, the agent handling the case started doing putting all the pieces together utilizing his research he received from the victim at the other location. They accounts were opened after they left McConnell AFB, to include other victims that had similar circumstances. Once the credit card accounts were open and he received the cards, he made as many purchases as possible at times maxing out the credit cards. After a while Mr. Doe got greedy and started making charges in the local area and these weren’t little charges he would go to restaurant’s with large groups and buy everyone’s dinner. This put the suspect in the local area, due to other charges that were being made online out of state this was solid evidence that the individual was in the local area. After sometime the fact finder was gather even more information concerning the victims in the case, finding out that most of the victims used to be stationed at McConnell Air Force Base. The fact finder made an interesting find, out of all the individuals who could potentially have access to personal information would have to come from the command staff or the security manager. Once records and documents were reviewed and confirmed that all the victims were from the same base at some point in time the puzzle started to take form. Mr. Doe had a gold mine of information at his fingertips. Mr. Doe had enough information on everyone in the unit, enough information you could practically be the person. Utilizing physical surveillance Mr. Doe was caught on tape utilizing a fake credit card at a local restaurant, himself his family and numerous others, the bill came out to 245.00 which was the last time Mr. Doe utilized someone else’s credit. Mr. Doe was relieved of duty read his Miranda rights and was placed in custody for financial identity theft and grand larceny. A jury of his peers were selected, 6 enlisted and 6 officers. The case lasted about 1 months; the victims testified all 10 of them, each losing anywhere from 10-20 thousand dollars. Though the government reimbursed those individuals for the money they lost as well as punitive damages it still couldn’t repair the physiological damage that occurred while these innocent victims had their identities stolen.

**The conclusion**

In closing I’ve discussed the six methods that are essential in any investigation. I’ve explained them in detail and how they are used in an identity theft investigation that occurred at McConnell Air Force Base. I covered how each method was critical in identifying important information insuring that the right information was gathered by the fact finder. I explained the importance of the project manager and how imperative it is to have someone that is competent, organized and knowledgeable in many aspects in law enforcement. I examined how the information found by the fact finder was able to bring the puzzle together allowing them to discover Mr. Doe and bring him to justice. After 1 month of testifying the grand jury came back with a guilty verdict on all counts of financial identity theft and grand larceny. The judge, who usually hands down sentencing at a later date, already had his sentence set. Mr. Doe was sentenced to 11 years at Leavenworth correctional facility where he was reduced to an Airmen Basic and will not be available for parole until after he has served no less than 8 years. His wife who said she knew nothing of his wrong doings cried as the sentence was read, his kids stood there not knowing what was going on unaware that they wouldn’t see their father a free man until they finished high school. There was a mixed emotion in the room, some felt sad that someone father and husband was going to jail for a long time not because he killed someone or assaulted someone but for stealing a lot of money from innocent people who worked hard for their money. Innocent people who might have gone through hard times because someone decided they wanted to be greedy and take something that didn’t belong to them. The victims had mixed emotions, some were glad that justice was served other didn’t know how to feel because even though they may had some rough time due to the incident but they survived and the government reimbursed them. In the end the process worked and the guilty were charged.

Introduction

Computer crimes are as common as shoplifting these days, thousands of Americans are victims of identity theft and it doesn’t seem to be slowing down. The case involving Tom Doe involved identity theft and the use of critical information to steal identities. The individual’s identities were stolen from information obtained during information given to trusted individuals who thought their information was being utilized for an U.S Government Secret clearance. Tom Doe was able to steal numerous identities utilizing trusted information he was given. I will discuss Computer Crime Investigations to discover, the who, what, when, where and how he exposed and brought to justice. I will cover the investigation process and how utilizing the most powerful tool, “the internet” and how it’s America’s Achilles in the war against computer crimes.

**Computer Crimes Investigation**

Computer Crime Investigations is not only a growing concern for consumers but those in the workplace. When you give your information to your employer you are entrusting them with you identity. Your identity is established once you are born and the federal government assigns you a number, a social security number that identifies your face to your name. Your face to your name allows another person to recognize you as you. With computer crimes, anyone can be you as long as they have your critical information i.e. you’re DOB (Date Of Birth), SSN (Social Security Number) and any information that can tie you to you. According to the FBI, the average computer –assisted embezzlement nets 450,000, while a similar crime without the aid of a computer nets only 19,000, while this information is a bit dated those figures have tripled. (Ferraro, 2012) Identity theft is the end goal of criminals, it allows them to commit crimes, steal money or live the life as someone else. How this happens is where the consumer should pay attention, now with the case involving Tom Doe this is not valid. Tom Doe was entrusted with your critical information and he abused his power. In most cases this can happen within the coperate world, this type of crime is called coperate espionage or the insider threat.

Social Media, Online banking and Smartphones all methods and ways criminals can either access your information or gather information on you to steal your identity. Social media is America’s weakest link, American loves to share information, information they don’t realize are pieces to a bigger puzzle. One mans trash is another’s treasure is how I look at information, Banking institution and other on-line sites use that information to identity you as being you. Online banking is another example of ways criminals get a hold of your information, never ever access your banking online on shared wireless access points, hotels, internet cafes or any other place you are sharing a wireless access point. This will allow those who are computer savvy to access your information through your laptop or smartphone. Smartphones are little computers and within the next four years more people will own a smartphone than a tooth brush, though that statistic is both alarming and indicates where American and the human race hold their smartphones and personal hygiene is a bit disturbing. People need to treat their smartphones like they treat their wallet or purse, people have their lives in their and should protect it the same way. Most Smartphones have the ability to enable the device to require a 8-12 password, I understand that this may inconvenient you at times especially when driving, but you shouldn’t be accessing your phone while you drive anyways. This eliminates the possibility if your phone is lost or stolen your information wont be stolen, just the phone. Most smartphone has the ability to back information up automatically so the only thing you will be out is the cost of a new phone rather than all your personal information which is priceless.

Home and work computer use a another vulnerability that can be mitigated by the use of simple awareness technique that can be second nature and reduce the risk by 50%. Viruses, Worms and other villains that exist in the virtual computer world are like gangs in the street, they are easily avoidable and by properly preparing your self you can avoid be a victim of a one of these malicious tools. (Ferraro, 2012) There are simple steps to properly protect your computer just by following these simple steps:

* + Antivirus software and frequent updates
  + Regular automatic updates for all operating systems and applications
  + Firewalls
  + Blocking executable attachments to e-mail from entering networks
  + Deleting Spam
  + Careful use of free file sharing service (they are often use to spread viruses)

(Ferraro, 2012)

Computer crime investigation are usually precipitated by three things, 1, the discovery that information has been lost, stolen or corrupted, 2 employee, customer and vendor complaints 3, accounting, banking or business process irregularities suggesting a computer crime or the use of computers to commit a crime. (Ferraro, 2012) With the case of Tom Doe, we were notified by another OSI field office that there was a strong coincidence that the victims were stationed together at McConnell AFB. Though the information wasn’t stolen from the computers, Tom Doe was able to use the information to open up numerous accounts. Though this didn’t implicate Tom Doe, this information only indicated that that they were stationed together. Once we were notified we made contact with human resources in victims unit, they advised us that they did control their information, but it they weren’t the only one in charge of said information. A witness indicated that the unit security manager also had extensive access to members personal information. This is the first time we made contact with the suspect, he indicated he was the security manager for the last 5 years and that he was responsible for over thousands of personal over the last 5 years and does not remember victim’s names. We examined the type of information the security manager had access to but still didn’t have enough evidence, prove or motive to implicate anyone. Soon, we received a few more calls that other individuals have had their identities stolen and had similar information that they were at one time stationed at McConnell AFB. This trend was building quick and fast and all the indicators were pointing at the security manager. With no evidence or proof that this individual was utilizing individuals personal information to open up credit card accounts, we had to a covert investigation.

So we have assessed the situation, and now preparing and planning for the next step. Gathering enough information to bring the suspect up on charges of Grand Larceny and identity theft and numerous of other UCMJ (Uniform Code of Military Justice) charges. So not to scare the suspect from acting any differently we did not bring any attention to the suspect allowing him to continue business as usual. Since the individual is on active duty we were able to gather information on the individual. Where he lives, kids and marital status, Tom Doe is married with three kids. His wife is a registered nurse and all the kids are still in school. They did however drive nice cars and have a lavish life style. Either they lived fugal or something was just not right. Gathering the right information is crucial at this point for a couple of reasons. Being able to gather information tying the suspect and the individuals together and catching hopefully catching the suspect making a purchase utilizing a stolen credit card. Charges that were made were always made in different states making it difficult to get information due to law governing where the crimes were committed. We are assuming the credit cards were created online, but all the purchases were made in other states as well as delivered to P.O Boxes. Crimes that are committed on a computer can involve multiple states even countries; this is why it is very hard prosecuting individuals of computer crimes. Unlike physical crimes, they involve local police and local resources making it easier to prosecute those committing crimes. Tom Doe was creating stolen identities and making purchases in other states and having family members all around the United States picking up the items. This information was all based on assumption, since we had to work with different law enforcement agencies the process took way to long allowing the suspect to make other purchases in other states. We needed concrete evidence, so we decided to follow the individual locally and we got a break. The individual was utilizing the stolen credit cards to purchase meals in the local area. We not only caught the individual on camera but was able to verify that he used it and signed the receipt of the stolen credential.

Once we had the incriminating information against the suspect, we made an arrest. The information gave us prove and beyond reasonable doubt that he was utilizing individuals information to open credit cards online. He never used information on individuals that were currently stationed their but if they moved or got out of the military they were prime victims. He knew these individuals had good credit because when verifying your information for your security clearance credit worthiness was a part of the questionnaire, so he know that these individuals had great credit. He knew every aspect of their lives, SSN, residences for the last 10 years, mothers maiden names as well as spouses critical information. His actions were undeniably horrible due to the trust his victims had to place in him, knowing that these individual trusted him with information that can ruin their lives.

Once all the evidence was in and reviewed the case went before a judge and a jury of his peers. Tom Doe was tried, convicted and sent to prison for his actions, though the U.S military compensated those affected by Tom Does actions, they will never forget the frustration of know that someone stole something that was given at birth and used against them.

Prevention and education is important, though management could not control this incident due to the amount of information Tom Doe had access to, allowed management to carefully decide who would have this job in the future. Measures are currently being implemented due to severity of critical information security managers hold and the information they have access to. It is my believe that this position must have a stringent role in the unit and have an impeccable background. Identity theft awareness should be part your monthly training due to the amount of new tools and tactics the criminals are utilizing. Awareness and training is your best mitigation tool in fighting and mitigating identity theft. Identity theft only leads to other criminal activity to include cooperate espionage and insider threat.

Conclusion

Computer Crime Investigation are only effective due to the unawareness of those being affected. Tom Doe took advantage of information that those entrusted in him and abused it. He was successful for years allowing those to suffer because of his greediness. He is still currently serving his time in prison and will continue to serve for a couple more years. Computer crimes and identity theft is only the beginning when it comes to future crimes. The Cyber threat is upon us and according to the Federal Bureau of Investigation, cyber attacks could be the biggest threat to the nation's security at some point in the future, and could even pose as big as a risk as the threat from terrorist attacks. (Rice, 2012)

Ferraro, E. F. (2012). *Investigations in the workplace (2nd Ed).* Boca Raton, FL: CRC press.

Rice, S. (2012, March 1). *Agence France-Presse* . Retrieved from BI Chief Warns Cyber Crime on Par With Terrorism: http://www.google.com/hostednews/afp/article/ALeqM5gIRfWz6-nqzxSvZ2i-tO\_ErRqk9g?docId=CNG.6294270dd5f26542527b791472efef0c.c1

Al Schweitzer, R. D. (1998). *Financial Identity Theft.* Washington, DC: Federal Trade Commission .

Powers, R. (2012, July 22). *U.S Military*. Retrieved from About.com: http://usmilitary.about.com/od/justicelawlegislation/l/blucmj.htm