Southwestern College

Investigation in the Workplace

Security Investigation

Portfolio Assignment

Computer Crimes Investigation

Identity Theft

By

Samuel L Alva

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 didn’t bring any attention to the suspect allowing him to continue business as usual. Since the individual is on active duty we were able to find gather some 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 wasn’t right.