The Bill Blackwood
Law Enforcement Management Institute of Texas

CyberCrime Investigators: A Path To Certification

An Administrative Research Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Gary Spurger

Harris County Constables Office, Precinct 4
Spring, Texas
July 2007

ABSTRACT

The certification of cyber crime investigators through TCLEOSE is relevant to contemporary law enforcement because as we move rapidly into the Information Age our investigators need to keep in step with the advancing technological criminal. The purpose of this research is to show that as technology advances so does the need for our investigators to acquire the special skill sets needed to accurately and effectively investigate high technology crimes.

The method of inquiry used by the researcher included the review of numerous journals and periodicals, articles, personal experience, interviews with seasoned cyber crime investigators and forensics specialists, and through the use of surveys. The researcher also had the opportunity to speak personally with administrators who have oversight of investigators. Two surveys were provided, one was provided to law enforcement administrators/supervisors and the other a phone survey of 30% of the state licensing boards for law enforcement officers around the nation. Each State has an organization that provides direction and credentialing standards for their respective law enforcement officers within their state. The researcher discovered that the surveys showed an affirmative response for the need to train for cyber crime while in the academy and to also provide a post certification process for investigators wishing to extend their knowledge beyond the basics. It was discovered that only 17% of the states in the nation provide any form of training in the fastest growing segment of crime in their academies and none provide a standardized post graduation certification process.

TABLE OF CONTENTS

INTRODUCTION

Computer Crime, also known as Cybercrime can be defined as:

> criminal activity involving the information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud. (Wikipedia Website, 2007)

The problem or issue to be examined considers whether or not there should be a standardized certification process for Cybercrime Investigators within the State of Texas that is maintained and administered by the Texas Commission on Law Enforcement Officer Standards and Education. This topic is separate from that of computer forensics. While computer forensics is an exacting discipline, there are many certification processes that are available for a “Certified Forensics Examiner”. The primary certifications are obtained and maintained by the Federal Bureau of Investigations and from many of the producers of computer forensics software packages that are currently available. This research is to be narrowly applied to the personnel who will be tasked with the initial contact and investigation with those persons filing criminal complaints.

A standardized certification process for Cybercrime Investigators is relevant to law enforcement because investigations of computer based crime, also referred to as

cybercrime, requires a specialized skill set that is not inherent to traditionally trained investigators. There are numerous complex laws that require special attention by the investigator to ensure that the proper method of legal request is utilized and that the proper information is obtained. Laws such as The Electronic Communications Privacy Act and the Privacy Protection Act of 1998 are not addressed in the Basic Peace Officer Certification Course. There are numerous state and federal laws that require special attention. When faced with dealing with the special circumstances of digital evidence in relation to acquisition and preservation there are specific requirements of law enforcement investigators.

The purpose of this research is to determine if the Texas Commission on Law Enforcement Officers Standards and Education should enact a standardized certification process for Cybercrime Investigators as is done for Instructors, Firearms Instructors, and other specialty licenses bestowed by the commission. This research will also will examine whether this certification process be a mandatory certification for those tasked with investigating these types of crimes or should be voluntary for those investigators wishing to further their proficiency in a prescribed discipline.

The research question to be examined focuses on whether those who investigate computer based crimes should be specially trained and designated as certified Cybercrimes Investigators. Another component to the research question is do the skills and knowledge differ significantly from standard investigation methodologies that would require an officer to have specialized training and if the training would provide the

citizens of the State of Texas with consistent investigative methodologies, thereby increasing the possibility that the offense reported will be successfully investigated to it's fullest extent.

The intended method of inquiry includes: a review of relevant articles, internet sites, periodicals, journals, personal interviews and a survey distributed to 25 participants from a broad spectrum of agencies. These agencies include Federal, State, County and Municipal agencies and include line level supervisors to senior administrators. There will also be a phone survey conducted of a percentage of the state licensing boards within the United States in order to determine if any other state is providing cybercrime training within their basic peace officers certification course.

The intended outcome or anticipated findings of the research will show that there is an affirmative need for a standardized certification process in the field of CyberCrime. This is due to the extended knowledge base required by investigators for a successful outcome and to increase the level of service provided to the citizens of Texas. This would also show that through a standardized certification process the investigator would be able to limit the exposure to unnecessary legal repercussions for the State of Texas and the investigators department by being able to negotiate the volatile field of Cybercrimes.

The field of law enforcement will benefit from the research or be influenced by the conclusions because it will show that there is an affirmative need for a standardized skill set, identified and set forth as the basis for a certification of a Cybercrime investigator. This will provide the citizens of the State of Texas with the comfort that

should they have a ‘Certified’ cybercrime investigator, they are dealing with a person who has a strong working knowledge of the proper ways in which to investigate their complaint.

REVIEW OF LITERATURE

While examining the question of certification for those tasked with investigating cybercrime, it is important to review the unique situation that cybercrime poses to society. As we have moved from the industrial age and into the age of Information Technology, a whole new frontier has emerged as the area of choice for many new criminals and types of crimes. Stephens (2005), noted that the level of street crime has diminished and that a new more insidious form of crime has taken its place where offenders can be thousands of miles away. Stephens continues with the concept that in large part, future policing will be dependent on the complexity and sophistication of the society that is being policed and that policing is known as a traditionally ‘slow-to-change’ subculture. Law Enforcement is generally regarded to be one to two steps behind the criminal in the realm of technology. Fair (2005), notes that computer crimes, like many offenses, begin the same way, through the filing of a complaint or report to a law enforcement agency. It is normally a regular patrol officer and not an investigator that will make the first contact with a complainant who wishes to report some form of a Cybercrime. Fair also states that there is no doubt that good computer skills are essential for such an investigation.

Griffith (2003), believes that a good investigator can be turned into an excellent investigator of cybercrime. Griffith believes that it would be much easier to teach

someone who is a good detective the skills necessary to investigate a cybercrime instead of taking someone who is a technology oriented person and teach them how to be a good investigator. This would validate the concept of teaching our current crop of detectives how to investigate cybercrime as the natural curiosity is already within the person to dig deeper and find the truth and to use his intuition and not just a technologist attempting to fix a problem. Griffith goes on to state that the bad news for investigators is that the records relating to cybercrime is digital information and has a finite existence so that the Cybercrime investigator had better act quickly to obtain and retain this information. There is no law requiring companies to retain data relevant to items connected to a Cybercrime such as connection information. Most agencies don't have personnel who are even remotely on top of what needs to be accomplished in order to obtain and retain data effectively in connection with a Cybercrime case.

In the field handbook titled "Cyber Crime Fighting, The Law Enforcement Officer's Guide to Online Crime" Spiropoulos (1999), states that chasing a crook through cyber space is nothing like the classic chase scenes in the movie "The French Connection". You have a whole new set of questions that need to be asked along with new clues and a myriad of new rules that govern the way we collect and preserve data for evidence. The guide book, which is printed by the National Cybercrime Training Partnership has an interesting disclaimer on the front cover:

> This is an introduction to the online world and the types of crimes committed there, online investigations, and the procedures for seizing and preserving computer evidence from the crime scene to the evidence room. But this book does not do several things. It does not make you a computer expert. It does not

> make you a computer forensics specialist. It does not prepare you to work pro-actively in the online world where undercover officers patrol the internet looking for criminals. (n.p.)

It is important to understand that it takes formal training and education to prepare an officer for a successful investigation that does not cross legal lines. Should the investigator cross these legal boundaries, it could place the prosecution of the offender in jeopardy. In the hand book it is noted on several different pages and under many different headings that many of the different Internet Service Providers, or ISPs as they have become to be known, that need to be contacted during an investigation in order to preserve data. While looking at the lists, this researcher noted that they are not correct due to recent mergers or acquisitions by other telecommunications providers. This issue, the dynamically changing landscape of providers, makes it difficult for the investigator who is not normally dealing with Cybercrimes to stay on top of who and where to send requests for information. With the laws surrounding the accepted methods of obtaining information changing with each contested court case, it becomes a daunting task to keep up to date with current requirements. There is a small section on page 16 that provides a general recommendation on the types of legal documents required to obtain specific pieces of information relevant to the investigation.

Casey (2000) tells us that as law enforcement officers, attorneys, and computer security specialists become more adept with computers as a source of evidence, the expectations regarding the collection, processing and retention of the evidence are becoming increasingly circumspect. This is due to few investigators being well versed

in evidentiary, technical, or legal issues surrounding digital evidence and as a result the digital evidence needed is often overlooked, incorrectly collected and not analyzed to any prescribed standard. This places the possibility of a successful investigation in extreme jeopardy. Casey also goes on to further identify Cybercrime as a crime that involves computers and networks and includes crimes that do not rely heavily on individual computers. He makes the point that the term has been generalized so it may also include crimes where a computer was not used to commit a crime but the network may still include digital evidence. This further makes it difficult for the average police investigator to track a criminal without the proper training and therefore the investigator must rely on the support of a private organization to collect the digital evidence. A "Cybertrail" has the possibility and probability of being great sources of digital evidence that include web pages, sent and received emails, stored images, digitized audio/video files and the ever important logs of chat conversations between the complainant and the suspect.

During the most recent Internet Crimes Against Children Conference in Dallas Texas (August, 2006) this researcher obtained a copy of the booklet titled "Internet Sex Crimes Against Minors: The Response of Law Enforcement" (November 2003) written by J. Wolak, K. Mitchell and D. Finkelhor. In this booklet they note because this is a new area, referring to sexual exploitation of minors perpetuated through the internet, the question arises as to whether these crimes pose particularly challenging obstacles for successful prosecution. They further state the diversified and multi-jurisdictional nature of law-enforcement activity in relation to these crimes has several implications. State and local law enforcement agencies, many without perhaps the specialized training to

investigate these offenses, are being called on to respond to internet sex crimes against minors. Because many of these cases require multiple agency involvement, an important part of any training for the investigators needs to include coordination and management training such as is provided by the Internet Crimes Against Children Task Forces training programs. These Task Forces are managed by the United States Department of Justice and the training is provided by the Fox Valley Technical Institute in Wisconsin.

Reading through a recent issue of the “Informant”, a periodical that is produced and printed by the National White Collar Crime Center for February 2007, there is a prominent article about online Auction Fraud. Maddox (2007) asserts that cyber criminals involved in online fraud take advantage of the complexity of the crimes they are committing. Some of the problems he associates with online crime is as the complexity grows there are inherent delays in obtaining needed evidence. He tells us that the investigator is now faced with a global neighborhood in which we must start looking for the suspects of these crimes. The periodical lists a training schedule for a number of courses designed to help the investigator learn to deal with online crime in a number of different areas. The classes are targeted at investigators wishing to learn more about forensics, basic cybercrime investigations, and many other topics of an online nature. While all the topics listed in the course offerings are aimed at online investigations, they are divided into specialties such as forensics, investigations, financial fraud, financial crimes against seniors, ID theft training and crime and terrorism. There appears to be no “certification” process listed for an overall understanding of cybercrime as a discipline. There are also many more articles in the

periodical that are focused towards the investigator who is already moderately computer adept and understands technology. These include articles on Stegonography, Internet Coin Fraud and Online Tax Fraud. There are also classes that use the computer in association with the title of Certified Forensics Examiner which is outside the scope of this research.

While there are thousands of experienced investigators on the streets of Texas, few are taught to deal with the technical aspects of digital evidence. They are not taught to deal with the complexities of conducting multi-jurisdictional investigations that tie in many law enforcement agencies and private sector entities. The private sector entities, such as financial companies and technology based vendors, are normally much more advanced than even the most progressive law enforcement agency. There is no current course curriculum or presentation within the law enforcement academies for our cadets on the intricacies of cybercrime investigations.

There are also issues related to the writing of search warrants as pointed out by Hickman. Cybercrime investigation warrants are often substantially longer because they must include a large number of definitions and explanations of technology that relate to the case. The information that is included in the warrants are normally very technically oriented and require a “dumbing down into layman’s terms”. This is in order for the judge who the warrant is presented for signature, will understand the reasoning and methods by which the investigator reached his probable cause for the warrant. (R. Hickman, personal communication, June 5th 2007).

This researcher had the opportunity to speak with Special Agent Jeff Chappell of the Immigration Customs Enforcement “Cyber Squad” based in Houston Texas and he

made a very important point during our discussion of this topic. Chappell said that as cybercime is being investigated from the initial complaint, the prosecution phase of the case has to be considered very carefully. It must be processed concurrently as the investigation phase so that the evidence can be collected in the proper sequence ensuring the prosecution has the evidence in a timely manner. This is vitally important as the evidence has a finite lifespan when conducting investigations that concern networks and logs of connection information. Log data shows actions such as connection information to a specific computer, the upload and download of files and possibly the transmission of specific files. These items are normally retained by Internet Service Providers. These logs are not always retained in the same manner by every Internet Service Provider and unfortunately, there is no set standard on what data is required to be retained nor for what period of time. Internet Service Providers do not maintain this information for a long time. In some instances, the logs are only maintained for several days. Additionally, some organizations such as college campuses and school districts only compound the issue of getting to the suspect. This places a very real time constraint on the investigator to obtain the data.

Another issue, Chappell stated, is the limited education in the area of cyber crime of the District Attorneys and Judges involved in the prosecution of the case. It is not uncommon that the investigator must spend valuable time in detailed explanation of the technological aspects of the case to the prosecuting attorneys. While investigators are normally very adept at basic law enforcement investigations and the legal aspects of the enforcement and apprehension of suspects, they must also be adept trainers and very good communicators. The investigators need not only be well versed in the

enforcement side of the legal equation but also be up to date with the legal precedents and court cases that affect how a case is presented to a prosecutor and regularly, this is incumbent upon the person actually doing the investigation as they are the one that is civilly liable if something is not completed correctly. (J.Chappell, personal communication, July 21, 2007).

METHODOLGY

The research question to be examined considers whether or not there is a need within the State of Texas for the certification of cybercrime investigators. Specifically, is there a need for specialized training in order to investigate a crime that involves computer technology beyond the normal investigative skills of the every day street officer/investigator. The researcher hypothesizes that there is an obvious need for a certification process for those investigators that are specifically tasked with investigating cybercrime. This researcher also hypothesizes that the skills needed to investigate cybercrime are somewhat specialized and are not included in any formal training provided by the State of Texas.

The method of inquiry will include the review of multiple articles, periodicals and journals. This researcher also conducted several interviews with investigators and forensics specialists. There are also two separate surveys associated with this research. One survey was distributed to law enforcement administrative/supervisory personnel tasked with investigations and case management. One survey was a phone survey involving a random sampling of state licensing boards to determine what certification or training they offer in reference to Cybercrime.

The instruments that will be used to measure the researcher's findings regarding the subject of Cybercrime certification will include both a written survey and a phone survey. The size of the survey will consist of 8 questions, distributed to 25 survey participants from many different law enforcement agencies within the state of Texas. The second phone survey consisted of only two questions and was provided to a random sampling of States that were picked through a random selection process performed by computer. The number of States sampled was set at 15 States, or 30% of the recognized licensing boards for Peace Officer Standards and Training, within the United States.

The response rate to the survey instrument resulted in showing the number of States that are actively taking a role in teaching aspects of Cybercrime. The response to the individual survey resulted in showing the number of agencies that have investigators assigned to Cybercrime investigations and displayed the administrators feelings toward the teaching of Cybercrime in the course requirements for new police cadets. The information obtained from the survey will be analyzed by showing the percentages of States that provide some form of formal education for Cybercrime and showing the representative percentage of agencies desiring some form of certification for investigators that they feel have acquired a formalized education in the investigation of Cybercrime.

FINDINGS

As the researcher reviewed the periodicals and journals it was found that it is a generally accepted fact that the law enforcement community is several steps behind the criminal element in our society. Many different authors find that as the more traditional

street crime has started to decline, the criminal element has thrived. The researcher learned through the criminology session taught during Module II of the Law Enforcement Management Institute of Texas, that the UCR has no means by which to track the increase in crimes involving computer related technology. There is no method by which to track identity theft, the sexual exploitation of children or financial crimes against the elderly through a nationalized system.

It was noted that there are many different categories of computer crime that include but are not limited to; fraud, identity theft, improper photography or videography, cyber harassment, breach of computer security, financial crimes against the elderly, and auction fraud. Sexual exploitation of children is a pervasive problem that includes things such as the creation, production, possession and distribution of child pornography, the online solicitation of children online and sexual assault facilitated by online communication. Each one of these crimes have things that are common and yet, things that are very different. The common factors are what we are most concerned about.

This researcher had the opportunity to spend time and interview Constable Ron Hickman, Harris County Constable, Precinct 4. Constable Hickman is currently on the National Steering Committee for the Regional Computer Forensics Labs that are charted by the Federal Bureau of Investigation. Hickman is also the chief administrator with oversight of one of the first dedicated cybercrimes unit in Harris County. Hickman noted that the kinds of documentation needed for the successful prosecution are vitally important as they are not intuitive to the regular investigator. Items such as a 2703d letter that can be sent by an investigator to an Internet Service Provider requiring that

provider to locate and maintain some form of data until a court order or search warrant can be secured to have that provider turn over the data as evidence. How a court order is needed for what is termed “Live Data”. Items such as email sitting in an email account and when a Search Warrant is needed to look into the evidence which may be contained in a suspect’s computer.

Through personal experience investigating Cybercrime, this researcher learned data maintained by an Internet Service Provider is very time sensitive. For example, when an email is sent or received, there is a time assigned as to when the email passed through the first server on its way to reaching its destination. This time designation is specific because the server may not be sitting in the same time zone as the investigator. The time has to be provided to the Internet Service Provider when researching a specific Internet Protocol address on a specific date and time. The investigator uses the time designation to identify the moment in time when the IP address was used and it must match correctly or the investigator will be getting inaccurate information in return. This is very important since from this single point of information, an investigator can either obtain a good search warrant for a location or getting a search warrant for the wrong location. It is vitally important to have the correct information.

In periodicals it was noted specifically that there are many instances where there is a need to cross jurisdictional boundaries in order to locate a suspect. In these situations, the investigator has to know how to properly provide the information to another agency and be tactful in soliciting their assistance. If the investigator can not accurately relay the needed information to another agency in order to further an investigation, there is little chance of a successful completion with successful follow

through for prosecution. It is imperative that investigators are educated on how to package information and case notes in order to effectively manage the case flow. There are instances and situations where the investigator will need assistance in order to obtain search warrants, location information and prepare case presentations.

One author notes there are circumstances where the investigator must move very quickly to preserve the data/evidence which is needed for the prosecution of the suspect(s). Most Internet Service Providers only keep data in a FIFO system (First In First Out). This means as new data is entered, the older data is deleted. Depending on the Internet Service Provider, the retention period varies widely. It is very important for the investigator to have the ability to discern what that duration is in relation to his investigation.

This Researcher had the opportunity to speak with Special Agent Jeff Chappell. SA Chappell is assigned to the Cyber Squad of Immigration and Customs Enforcement which is tasked with the investigation of online child sexual exploitation. SA Chappell states one of the more pressing issues with the investigation of cybercrime is most investigators do not start their investigation with the prosecution phase in mind. Unfortunately, when working a cybercrime, it is imperative to work a case with this phase in consideration from the very beginning. This is important because there are aspects of a cybercrime investigation that do not flow as do other more traditional investigations such as interactions with Internet Service Providers, cooperation with private entities that supply technology such as hardware needed to collect data, and privacy issues that are not adhered to. For example, the Privacy and Personal Protection Act of 1998 provides a means to allow the private citizen to sue an individual

investigator for not returning information protected by the act even when a search warrant was appropriately executed. The Electronic Communications Privacy Act governs the government's access to stored email. When conducting a cybercrime investigation, there is the possibility of exposing the investigator and the investigator's agency to litigation thereby adversely affecting the prosecution of the case.

While conducting research on the laws within the State of Texas concerning cybercrime, it was noted that even Texas law and court precedent do not always coincide and are fertile grounds for controversy. Take for example the recent court ruling that allows an arresting officer, prior to completing the booking process of a defendant, to look through the defendant's cell phone (United States v. Jacob Pierce Finley, January 26th, 2007) that is recovered on the defendant, for information such as other phone numbers and with whom the defendant has been communicating. In contrast, Texas law states that if anyone uses the computer, network or computer system of another without the owner's effective consent, they are in violation of the offense of "Breach of Computer Security".

By definition, a cell phone is a computer system and many cells phones, or PDA (Personal Digital Assistant) phones like Research in Motion's Blackberry or Motorola's Q which supply computer programs that are capable of editing documents, spread sheets and photographs. The later runs a version of Microsoft's software called Windows Mobile 5. This poses a significant problem for the investigator should he use the data located on the device without a search warrant. It was noted by Constable Hickman that defense attorneys are already working on ways to educate their

community about the uniqueness of situations such as these and how to use them to their advantage through collaborative websites and training seminars.

In discussions with SA Chappell and through personal experience, this researcher learned that once an investigation reaches the level of search warrant execution, it is imperative that the investigator is trained in appropriate search techniques. When executing a search warrant in relation to a cybercrime, there are technology issues that must be addressed to successfully conduct the search. Is there an open Wifi network in the location? Are there Wifi enabled devices secreted in the location? Who is trained in the proper recovery of computer equipment and what kinds of operating systems are in use? What kinds of questions are asked during the suspect interview? These are just a couple of the numerous issues that must be faced by the investigator, not to mention where does the hardware go for processing and who will complete the forensics exam.

In speaking with Detective Lawrence Potier, A Certified Forensics Examiner for the Greater Houston Regional Computer Forensics Lab, and through this Researcher's personal experience, communication with the personnel assigned to perform the forensics exam is vitally important to the investigation. If the investigator does not effectively communicate what is sought, the forensics examiner does not know what or how to look for evidence. This information relates together with the timeliness of the data recovered, the items recovered at the location of the search warrant, information supplied by the Internet Service Providers and finally the questions that are asked of the

suspect during the interview. All of it comes together to provide the forensics examiner the information he needs to narrow his exhaustive search of the digital data on the recovered computer devices.

Based on the information learned through experience and research it was deemed appropriate to ask, based on a random sample, how many States are teaching components of cybercrime to their new cadets and if those States are providing any form of certification process for investigators who conduct cybercrime investigations. A random sample of States was compiled and showed that only 17% (see figure 1) of the surveyed State licensing boards provided any form of cybercrime training within the Basic Peace Officers Course and that none of them provided any form of post academy certification ensuring an officer had a sufficient skill set to investigate cybercrime. When talking with Mr. Breuer of the Utah POST (Peace Officers Standards and Training) Commission he stated that the State of Utah did not see the need for a cybercrime course as it was not an issue in their state. After further conversation, Mr. Breuer realized that his office should revisit the concept in the very near future. This researcher also had the opportunity to speak with Commander Fyfe with the New York City Police Department's Police Academy and learned that New York City PD does not fall within the jurisdiction of the state licensing authority. Commander Fyfe stated that the State does not teach cybercrime in the State academy but the NYPD does teach a component of cybercrime investigation in their Basic Academy encapsulated within the crime scene search.

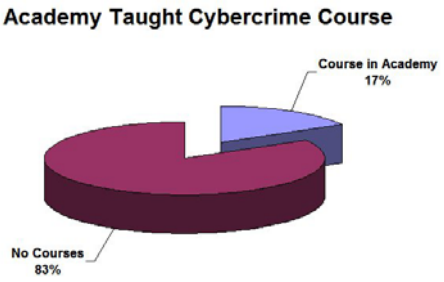

Fig 1. Ratio of States that include courses on cybercrime within their Peace Officers Academy.

A survey of law enforcement administrators (see Fig. 2) from around the State of Texas and academicians within the LCC was conducted. The primary questions asked where should TCLEOSE teach an educational block on cybercrime and should there be a certification process for post academy graduates. This researcher found that the respondents to the survey, 25 in all, provided insight as to the growing trend towards the realization that training in this area should be more prevalent and profound. Of the respondents, the survey showed that 20 agencies have personnel dedicated to performing criminal investigations and seven agencies have investigators dedicated to cybercrime. It was noted that of the 20 agencies that have investigators, nine agencies have personnel trained in cybercrime investigation in one form or another. While 23 of the agencies responded that they felt training would help in the prosecution of cyber criminals, all 25 showed an affirmative response that TCLEOSE should include a module in the basic peace officer academy dedicated to the issue of cybercrime. There were 23 agencies that agreed that there needs to be some sort of post graduation certification for cybercrime investigators, 15 of those agencies feel that the certification should be voluntary while seven feel that it should be a mandatory form of certification.

This information is significant, in that 100% of the respondents feel that there should be TCLEOSE mandated education in the academies.

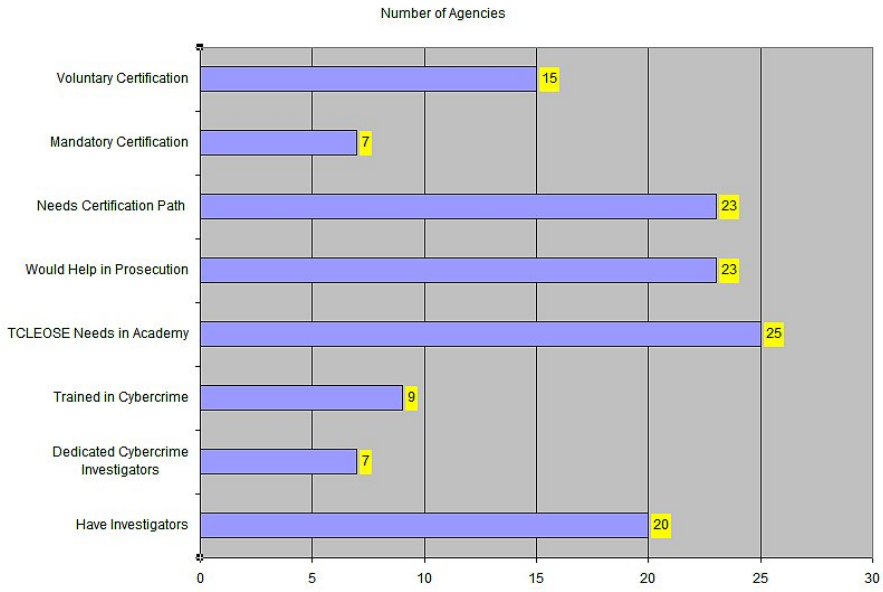

Fig. 2 – Results shown from the survey of law enforcement administrators located in Texas.

DISCUSSION/CONCLUSIONS

The problem or issue examined by the researcher considered whether or not the State of Texas should provide a pathway for an investigator to become a certified cybercrime investigator as set forth and maintained by the Texas Commission on Law Enforcement Officers Standards and Education. Also examined was if TCLEOSE should provide an educational component within the basic peace officers academy for the investigation of cybercrime.

The purpose of this research was to demonstrate how complex and complicated the issues surrounding a cybercrime investigation can become and how under prepared our investigators are within the State of Texas. This is primarily due to the lack of training provided by the State of Texas and the need for assistance from TCLEOSE to enact a standardized training course for investigators. The research question which was examined focused on some of the problems encountered by investigators when involved in investigating a cybercrime. They are numerous and complicated and are forever changing in legality. The problems require specialized training in legal aspects and in respect to the numerous kinds of digital evidence that may be present at any crime scene.

The researcher hypothesized that investigators in the State of Texas are currently not in step with technological trends in a general sense. Also expected was that there is not a prescribed standard for how to work a basic Cybercrime investigation. The researcher concluded from the findings that there is a definite need for more training for investigators of cybercrime and that a certification process would be beneficial to ensure that investigators have a basic knowledge necessary to conduct a successful investigation. There also appears to be widespread support for such a certification among law enforcement administrators.

The findings of the research did support the hypothesis. The reasons why the findings did support the hypothesis are due to the fact that cybercrime is an increasing problem in society today and because the nature of the investigations is becoming more complex. Due to this increase in complexity, specialized training is needed to keep up to date with the technology to ensure that the investigator does not expose the

department or the investigator to unnecessary litigation. Limitations that might have hindered this study resulted because technology is dynamically changing from day to day and the laws involved are constantly being tested. The technology that was current yesterday is already outdated tomorrow.

The study of cybercrime certification is relevant to contemporary law enforcement because the public we serve and the administrations each investigator works for stands to be benefited by the results of this research because it will provide a starting point, through certification, where all investigators and newly trained police cadets may start their investigations. Law enforcement will be better suited to provide a higher level of service with the possibility of a successful prosecution and a successful resolution of the complainant's case.

REFERENCES

Cybercrime (2007, July). Cybercrime Definition. Retrieved July 19, 2007, from http://en.wikipedia.org/wiki/Cybercrime

Stephen, G. (2005). Policing the future, law enforcement's new challenges. *The Futurist,* March-April 2005, 52.

Fair, R. (2005). Feasibility of a cybercrime investigations unit in a police department. *The Bill Blackwood Law Enforcement Management Institute of Texas.* November 2005, 6-7.

Spiropoulos, J. (1999). *Cyber crime fighting – the law enforcement officer's guide to online crime*. Fairmont, West Virginia: The National Cybercrime Training Partnership

Wolak, J., Kimberly Mitchell, David Finkelhor (2003). *Internet Sex Crimes Against Minors: The Response of Law Enforcement*. Durham NH: National Center for Missing & Exploited Children.

Maddux, R. (2007). Online auction fraud: from caveat emptor to caveat venditor. *Informant*, 2(3),23.

APPENDIX/APPENDICES

CyberCrime Investigations Survey

This survey is designed to elicit information relevant to an Administrative Research Paper for the Bill Blackwood Law Enforcement Management Institute of Texas. Your responses are greatly appreciated. If you have any questions, please ask.

Cybercrime defined:

"Cybercrime is a crime committed against a computer or by means of a computer. Harm resulting from such crimes can be to property, to persons, or to both. There are also politically motivated crimes, controversial crimes and technical "nonoffenses" in the cybercrime world (Brenner, 2001 a,b)"

Schell, Bernadette H. (2004), Cybercrime: a reference handbook, ABC-CLIO

What is your type of agency?

[] Municipal [] County [] State [] Federal [] Other

Does your agency have a person(s) dedicated to Investigations?

[] Yes [] No

Does your agency have a person(s) dedicated to investigating Cybercrime?

[] Yes [] No

Do the investigators have specialized training in the area of Cybercrime?

[] Yes []No

Do you feel that TCLEOSE should add a module in the basic academy a section on Cybercrime?

[] Yes []No

Do you feel that a Certification process that teaches the necessary skills to investigate Cybercrime would better provide the possibility of prosecution of a defendant?

[] Yes []No

Do you feel that there is a need for a Certification Process for Cybercime Investigator as there is for Computer Forensics Examiners?

[] Yes []No

If yes, should it be mandatory or voluntary for the officer to obtain?

[] Mandatory [] Voluntary

Thanks for your assistance –

Sgt. Gary Spurger
Tech Services – Computer Crimes Unit
Harris County Constables Office, Pct 4
Gary_spurger@cd4.hctx.net

State listing for the random state survey. The states that were randomly chosen using a random number generator are shaded in gray. Notations are then placed in the fields for if there is training provided in the States basic police officers training, how many hours are dedicated to it in the academy and then if there is a separate certification process for Cybercrime investigators.

	State	In Academy	# of hours	Certification
1	Alabama			
2	Alaska	No	0	No
3	Arizona	Yes	2	No
4	Arkansas	No	0	No
5	California			
6	Colorado	Yes	2	No
7	Connecticut			
8	Delaware			
9	District of Columbia			
10	Florida			
11	Georgia			
12	Hawaii			
13	Idaho			
14	Illinois			
15	Indiana			
16	Iowa			
17	Kansas	No	0	No
18	Kentucky			
19	Louisiana	No	0	No
20	Maine			
21	Maryland	No	0	
22	Massachusetts			
23	Michigan			
24	Minnesota			
25	Mississippi			
26	Missouri			
27	Montana			
28	Nebraska			
29	Nevada	No	0	No
30	New Hampshire			
31	New Jersey			
32	New Mexico	No	0	No
33	New York	No	0	No
34	North Carolina			
35	North Dakota			
36	Ohio	Yes	4	No

37	Oklahoma			
38	Oregon	No	0	No
39	Pennsylvania			
40	Rhode Island			
41	South Carolina			
42	South Dakota			
43	Tennessee			
44	Texas	No	0	No
45	Utah	No	0	No
46	Vermont			
47	Virginia			
48	Washington	No	0	No
49	West Virginia			
50	Wisconsin			
51	Wyoming			