The Bill Blackwood
Law Enforcement Management Institute of Texas

==========

Feasibility of a Cybercrime Investigation Unit in a Police Department

==========

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

==========

By
Robert C. Fair Jr.

Sherman Police Department
Sherman, Texas
November 2005

ABSTRACT

Each year millions of American are victimized by computer crimes and are not even aware that the crime has occurred until months after the incident has occurred. With this massive amount of crime taking place over the internet a growing concern is how are police department reacting to this epidemic. This study examined the various categories or levels of computer crime, and then focused on computer crime at a local level. The research identified some of the many crimes that involve the computer as well as the problems of implementing a new program into a department. The purpose of this study was to examine the feasibility of a cybercrime unit within a police department. Research of relevant published materials, interviews, and surveys of other agencies aided in identifying current trends, successes and failures other departments have experienced in dealing with cybercrime investigations.

Research indicated that while most police departments did not have any special investigative unit that investigated cybercrime. Most of the agencies that did examine cybercrime had the criminal investigation unit look into major cases that affected them. Only a small percentage of the departments actually had a special division to investigate cybercrime cases.

With technology continuing to advance so will cybercrime. Police departments are already behind in the investigation of these crimes. While all agencies may not need to know how to complete the forensic analysis of a computer, we all do need to know how to investigate computer crime and the resources at our disposal. The research in this paper has identified several options any department may use to investigate computer crime and resources available to departments.

Table of Contents

Page

Introduction

With the age of technology came an awakening with the realization of how much the computer plays a role in our daily lives. Along with the benefits of the computer, however, a negative aspect associated with the computer age came the criminal element known as Cybercrime which breaks down into three categories. The first category is crime in which the computer is the object of the attack such as viruses that are sent to infect other computers (worms). The second category is where the computer is a tool used to commit an act against another such as applying for credit cards in somebody else's name or hacking into a computer. Third, the computer is an incidental part of the crime. An example of this is the pedophile that finds his victims by using the computer.

There are also several levels of crime that must be examined as well. Cyber warfare can be an international crime that involves computers. A recent example is the recent power outages that occurred across the United States in August 2003. The concern was whether it was merely an equipment failure or possibly the work of a terrorist organization preparing for another attack on this country. While this is interesting this research is mainly concerned with Cybercrime occurring at the local community level including theft, identity fraud, credit and debit card abuse, child pornography, pedophiles, stalking, contraband purchases and many more. The perpetrator committing the act is only limited by his imagination as to the list of crime he or she can commit.

Local agencies need to combat this ever-growing problem. The question to examine is; should the Sherman Police Department create a cyber crime division to investigate these types of crimes? The intended method of inquiry that will be used to examine this subject will include researching written data on the subject, books,

periodicals, and magazines. A random survey will be conducted to see what other agencies are doing to address this problem. The final method will be to visit departments who currently have a cyber crime unit to see what other pertinent information can be gathered.

The intended outcome of this research is to assist the Sherman Police Department on deciding whether the department should form a cybercrime unit. The problem, as outlined, would appear to indicate that the department should form the unit. There are other issues such as manpower, financing, and location of the unit that need to be answered before a true decision can be reached. Another issue to examine includes whether or not the department and the county could be better served with a cybercrime task force. With the creation of a cybecrime unit officers are better enabled to work with different departments together to solve these offenses. One distinct advantage to organizing a task force includes agencies sharing information and having an avenue to investigate these crimes. Cybercrime does not know borders and crosses from one jurisdiction to another. With every program, and especially one that involves multiple agencies, there are numerous problems to examine as well. Many of the problems a single agency faces are similar to that of a task force including manpower, financing, and, when numerous agencies become involved, the problem of supervision.

The problem of cybercrime is not going to go away. In fact with the advance of technology the problem will continue getting worse. A look at this problem will help determine if the Sherman Police Department needs to develop a Cyber Crime unit or if a task force is needed to combat the problem in the community.

Review of Literature

Previous research and the current paper shared one consistent factor; cybercrime is here to stay and will continue to grow as long as we continue to grow in technology. Our police department like many others in the country have seen the level of crimes committed with the computer soaring. Fraud, crimes against children, and many other offenses that we have never dealt with in the cyber world, are now in our own backyard. Griffith (2003) covers a story on the proper way to investigate cybercrime. This is a crucial element in answering the question if we at the Sherman Police Department should create a cybercrime unit. It is imperative to first understand how to approach a cybercrime investigation so that certain elements of the offense are not overlooked. Griffith first dispels the perception that you have to be a computer geek in order to investigate computer crimes. He states "A lot of the best cybercrime investigators are just local detectives who have branched into a new field" (Griffith, 2003, p.18). Griffith advises that any experienced investigator can become an excellent cybercrime detective. He believes it is much easier to teach a good detective how to investigate computer crime than try to teach someone with computer skills how to be a detective. However there is no doubt that good computer skills are essential for such an investigation.

Computer crimes, like any offense, begin the same way with a complainant reporting the crime to the police department. One of the first steps in the investigation is to find the I.P. or internet protocol of the offender. An I.P. is a series of numbers attached to every piece of information sent out over the internet. This internet protocol attaches the user to their internet service provider, I.S.P. The I.S.P. documents everything the user

does on the internet. This is great news for detectives investigating offenses because it provides a trail of evidence for officers to follow.

The bad news is this information has a very finite existence. In other words the investigators wanting the information from an I.S.P. need to gather information quickly because the I.S.P. deletes information quickly, sometimes within a month, to avoid the cost of saving information for extended periods of time. Most internet service providers will work with the police and if a request is made for the information the I.S.P. normally cooperates with the department to hold information without a warrant or subpoena. Such records provide the identity of the offender. I.S.P. companies require personal information from customers when purchasing services. Investigators use the personal information to identify offenders involved in cybercrime. Just as in traditional crime offenders use false information to conceal their identities. Traditional means of investigation work to identify offenders who falsify information.

Another interesting note in the investigation of cybercrime includes how departments rely on each other for support. Cybercrime knows no boundaries and crosses from one jurisdiction to another, which forces departments to work with each other to put offenders behind bars. For example, when the crime actually occurs in Las Vegas but the victim is in Dallas, departments assist each other in serving warrants and subpoenas. Most departments are quick to assist as this means that their agency is not forced to complete the investigation in their town. Piazza (2003) points out that most police departments in the country are not on top of cybercrime and do not know how to investigate the cases. Like many other cities, the Sherman Police Department, only reacts when a crime directly affects a member of the community.

The information above deals with the investigation of the cybercrime itself. The second part of the investigation involves individuals analyzing the forensics of the computer system. These specialists are known as the experts in the cybercrime investigation process. The work is so specialized that most departments do not become involved in the process but rather farm out the forensic investigation to others. The basic concept is once the computer is in police custody a forensic specialist mirrors or makes what is also called a true copy of the hard drive. This copy would include deleted, temporary, and other data that could prove to be critical to the investigation. The mirrored or true copy would then be examined for the evidence in the case. The reason many agencies send this out for examination by other agencies is the expertise required in the review, and the cost for the equipment and software is very expensive.

Clifford (2001) believed that technology has brought us into a new age. Many of the crimes committed today would never have been possible without the new technology afforded by the computer. Hall (2000) stated "Law enforcement in America and internationally could be facing its biggest challenge as the amount of criminal activity online is soaring. It's formidable, intimidating, often anonymous and always' unruly. And while it maybe the Last Great Frontier for the optimist among us, to law enforcement, the internet is considered by many as the most daunting challenge of the new century and perhaps the most problematic policing issue in history" (p. 1). Hall believes that any crime that you can do on the street you can also do online including theft, identity fraud, and kiddie porn. He also confirms that this is a crime without borders that is increasing everyday. Hall agrees with Griffith's research discussing how high technology crime is the same old crime, just done with some form of electronic

technology. An indication of how fast cybercrime is soaring is to look back five years ago just examining a possible problem and needing to become prepared. Now the problem is occurring and the majority of police departments are caught unprepared to handle such cases. Last year statistics revealed a 42% jump in the number of complaints filed. The police response to these numbers, however, falls short. Law enforcement is outdated and no where near knowing what all is going on out there. Some of the larger agencies have created cybercrime units in their departments, but thousands of smaller department have yet to address the problem. The cost for equipment and training is expensive and smaller department's budgets cannot afford the expenditure. Hall like others states the three C's are needed collaboration, communication, and coordination at the local, federal, and international level in law enforcement is needed if agencies are going to have any success in fighting this problem. Law enforcement needs to get beyond the traditional turf wars and work together.

On a larger scale the CSIS task force report (1998) examined computer crime from a national level. The threat to information systems involves strategic information warfare. Such warfare is a direct result of information technology. United States officials discovered some attacks by hackers on their systems which is a step in the right direction. However, the attacks that are undetected are cause for concern. The objective of the suspect who hacks into the government information system is to wait and gather information and go undetected as long as possible. The greater danger with this scenario is that the attacker remains anonymous for an extended period of time and then at their choosing strike. The CSIS report (1998) referred to a computer type of Pearl Harbor. The purpose of the intruder remains unknown until it is too late.

Some of the main reasons indicated for any individual to hack into the governments or any major corporation's main frame include theft, destruction of the technology or information, to exploit or disrupt the service, or an ultimate goal of altering the role of United States in a political situation. CSIS report (1998) also points out that information technology is readily available in all levels including cybercrime. Private companies, not the government, now lead the way in information technology. With the deregulation of telephone and other information systems the ability to address the information warfare threat becomes more difficult.

The remaining articles reviewed all indicated the exact same problems with cybercrime including the increasing rate of occurrence, expensive training, and the need to communicate beyond traditional borders with other agencies (Lang, 2002; Piazza, 2002; Piazza, 2003). There is no doubt that law enforcement need to take drastic steps to try to keep up in the investigation of cybercrime offenses

Methodology

The purpose of the paper is to determine the feasibility of a cybercrime investigation unit in a police department. With the realization that computers are here to stay and what previous researches studies found the answer to the question is yes. Cybercrime is not going to decrease anytime in the future. As technology affords us the opportunity to do more online, the opportunity for the criminal to complete their task will also increase. However there is a lot of thought that must go into the decision making process concerning creating a cybercrime unit including the training, equipment, and manpower. Such factors are expensive which require departments to refigure their budgets to see if a cybercrime unit is feasible for their organization. Examining what

level of the investigation process in which the department enters is also a major factor to consider. While all agencies investigate cybercrime at some level, it is important to analyze the specific needs of the individual department.

To examine this issue the researcher reviewed relevant published information to discover current trends, problems and successes other agencies found. The researcher developed and distributed a survey (see Appendix A) to participants in Module I at Texas A& M University for a statewide perspective of the level of investigation other agencies are completing to address this problem. Then officers of the North Texas area attending local classes completed the survey to determine what local departments were doing in the local area.

The researcher then made contact with the United States Secret Service office located in Dallas, Texas as well as the North Texas Regional Computer Forensic Laboratory, which is affiliated with the Federal Bureau of Investigation to see what services they provided to police departments and assistance they offered with this research.

Findings

The agencies survey (see Appendix B) ranged in size from very large police departments, to agencies who only employed a handful of officers. Forty surveys remained after separating duplicate responses from agencies. Of the 40 responses 63% advised that they did not have a cybercrime investigating unit in their department at all. Twenty-two percent advised that the criminal investigation division completed investigation of computer activity. Fifteen percent of the personnel surveyed advised that they did have a full computer crimes unit in their agency. The 15% or the six

departments that identified that they did have a division assigned for the investigation of computer crimes included police departments located in the bigger cities in the State of Texas (see Appendix C).

The researcher contacted the United States Secret Service office to inquire about the services provided for the Sherman Police Department. On several cases our agency became involved in dealing with pedophiles that were using the computer to receive pornographic images of children. Our family services office contacted the Secret Service and they completed the forensics on the computer and obtained the necessary evidence to assist in getting the conviction on the suspect.

The researcher met with Robert W. Sheffield (2005) at the Dallas office of the Secret Service. The researcher inquired about the services they offered police departments and asked if and why smaller agencies needed to form a Cybercrime Unit. He advised that technology is only going to continue to grow and become more prevalent in today's world. The current research identifies the computer as a resource that more and more criminals are using to commit their crimes. Sheffield pointed out that investigators lose valuable information and evidence because detectives are unaware of the value of the computer's hard drive. Sheffield explained that when the focus of the crime is not the computer as in a homicide investigators often overlook the evidence that is possibly on the hard drive. They see the physical evidence of the crime before them but often overlook the computer. The computer could possibly contain key evidence which could secure a conviction in the case. Examples of information recovered include researching websites a suspect viewed to find out how to cover up a murder, emails the suspect sent before or after committing an offense, and discovering who the suspect

communicated with about the offense. In narcotics cases the emails sent between suspects involved in narcotics trafficking can assist in building the links for a conspiracy case or finding other distributors in a possible dope ring. As shown, the information that remains at the scene, long after the investigators leave, is critical evidence towards securing a warrant for an arrest.

The information or evidence obtained from a computer is also excellent information for the prosecutor of any case. This information is extremely difficult for a defendant to refute because the information is contained on his computer. The information is identified by date and time to indicate when the defendant communicated with others. If the suspect attempts to manipulate or delete the information after the suspect is aware he is the subject of the investigation, this activity shows that the suspect is intentionally trying to conceal the illegal activity. Another great advantage of the information obtained from a computer Sheffield advised is that most computer evidence or information is rarely contested in court. Due to the strength of the evidence the defendants rarely go to court on a case. The information is irrefutable and the suspect normally takes a plea agreement and never sees a courtroom.

The researcher also inquired about what other services the Secret Service offered local police agencies. Sheffield advised the availability of forensic analysis of the computer through federal funding for cities to assist in the investigation of computer crime. The Sherman Police Department asked for assistance in the past from the Secret Service and other federal agencies concerning the completion of forensics on computers. Sheffield also advised that the Secret Service offers a program to allow willing departments to enter into an agreement that allows for training and equipment in

exchange for services. Sheffield indicated that Dan Fletcher from the Addison Police Department is an excellent example of the benefits of working with the Secret Service. Fletcher observed that the Addison Police Department often overlooked offenses associated with computer crime. Fletcher requested control over such crimes to possibly investigate them more thoroughly. His department, seeing his interest, advised him to research the necessary training and equipment to investigate the cybercrimes. After learning the expense of running a cybercrime unit the department felt incapable of pursuing this avenue. Fletcher then researched the Regional Lab and found some road blocks there, including a three year commitment to work for the lab to offset the cost. Fletcher then came in contact with the Secret Service office and reached a deal that including training. Fletcher participated in the Secret Service Training which valued at approximately 80 to 100 thousand dollars worth of training and equipment. The equipment provided furnished offices at both the Secret Service and the Addison Police Department. In return the Addison Police Department agreed that Fletcher spent time assisting the Secret Service with their case load as well.

However this type of agreement sometimes leads to problems. Along with the computer cases Fletcher works other cases assigned at Addison which increases the caseload assigned to Fletcher. The agreement appears to work fine and the Addison Police Department as well as the Secret Service Office both win in the end. Agent Sheffield also advised that there are certain important tasks that need to address when starting a cybercrime investigation unit. First, look into taking forensic courses and become educated. Second, assure that the software programs you are using are certified as well. Make sure that your training and software meets American Society of Crime

Laboratory Directors – Laboratory Accreditation Board (ASCLD) certifications. The final thing is to set proper protocols in your agency to assure that the digital evidence you retrieve is good solid evidence that can be admissible into court. While this training and equipment is very expensive make sure the agency takes time to look outside the department budget for funding. Other areas to search for possible funding include the local Council of Government for funding set aside for cybercrime investigation.

Conclusion

The following research looked at the feasibility of a cybercrime investigation unit within a police department. There is overwhelming evidence to indicate that the problem of cybercrime is only going to continue to grown in the country and our cities. Previous research indicated that agencies are already behind in this area of investigation. If departments wait any longer the only ones who will continue to be hurt are the victims of crime and the reputations of our agencies. Just as law enforcement continues to evolve with sophisticated labs and methods of investigation, the investigation of cybercrime is the next steps our agencies need to take. Although not all agencies need the ability to complete the forensics of a computer, however, all agencies need the knowledge of the investigation process. The current research clearly showed the importance of the tools and resources that are available at their disposal. F.B.I. and Secret Service agencies provide valuable resources that are available to police departments for the forensic analysis of the computers. Investigators need to know that investigating cybercrime is just like investigating any other crime except you are in a cyber world. Agencies need to learn the in and outs of these investigations and then rely on the resources of others to assist us when we require them. To simply ignore these complaints hurts everyone. The

researcher identified possibilities for funding and education if department heads are willing to work through difficulties including funding, equipment and training, and diversity of cases. This is a give and take process with great advantages for any department willing to work with federal agencies. Research also indicates how far we really are behind in this endeavor. Sixty three percent of our agencies in the surveys indicated the lack of investigative units. It is important for all agencies to recognize the importance of investigating cybercrime.

After conducting the present research the Sherman Police Department examined the possibility of working with the Secret Service on cybercrime investigations. To answer the proposed research question concerning the feasibility of a department implementing a cybercrime unit, the researcher believes that at some level all departments needs to react to the growing number of cases involving cybercrime. The size of the unit varies by department, but all officers need a basic understanding of the elements of cybercrime investigation. It is the beginning of the road but remember "Nothing ventured, nothing gained". Once again law enforcement is changing and departments need to evolve.

References

Clifford, R (2001) Cybercrime: the investigation, prosecution, and defense of a computer related crime. Durham N.C. Carolina Academic Press

CSIS task force report (1998) Cybercrime—cyberterrorism—cyberwarfare; averting an electronic Waterloo D. C. CSIS Press

Griffith (2003) Police The Law Enforcement Magazine Nov 2003

Hall, D (2000) Logging on with a vengeance in the year 2000. Police Redondo Beach

Piazza, P (2002) Wanted: Tools, expertise to fight cybercrime. Security management Arlington

Piazza, P (2003) On patrol in cyberspace. Security management Arlington

Appendix A

Survey

1) What type of department are you employed in? (Circle one)

Municipality County ISD University Other

Department_____

2) Population of your jurisdiction? (Estimate) _____

3) Number of officers in your agency _____

4) Does your department have a Cyber Crime division or are you a part of a task force assigned to investigate cyber crimes?
(If neither please state)_____

5) If answer yes to #4 how many investigators are assigned to this task_____

If your agency can provide me with information on cyber crime investigation unit please leave names and numbers of contacts.

_____

Thanks for your assistance

Lt. Bob Fair
Sherman Police Department
903-892-7337
bobf@ci.sherman.tx.us

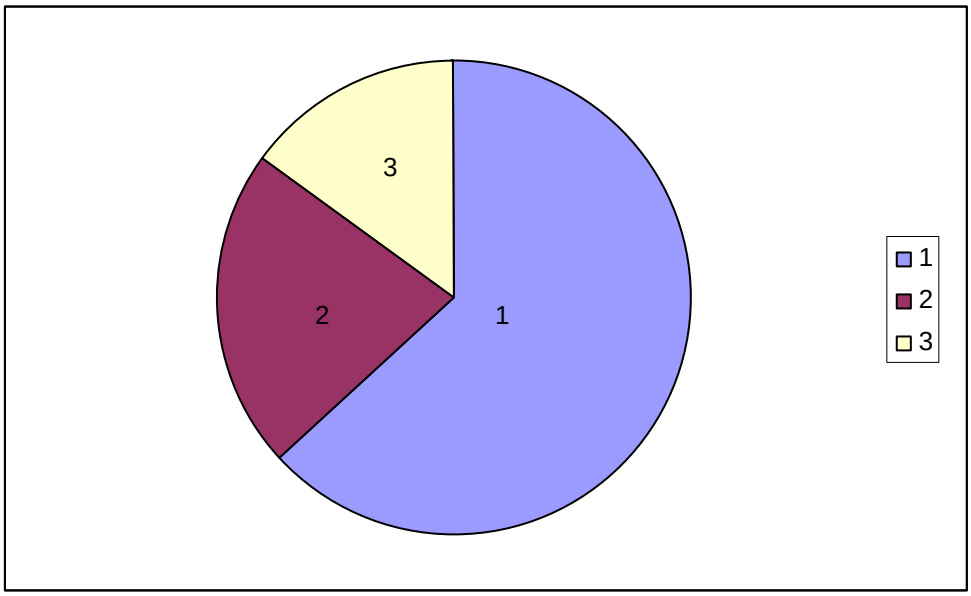
Appendix B

Departments Surveyed

1. Tomball Police Department
2. Corpus Christi Police Department
3. Department of Public Safety
4. Austin Police Department
5. San Antonio Police Department
6. Arlington Police Department
7. Denton County Sheriff
8. Comal County Sheriff
9. El Paso Sheriff
10. McKinney Police Department
11. Allen Police Department
12. Double Oak Police Department
13. Aubrey Police Department
14. The Colony Police Department
15. University of North Texas Police Department
16. Prosper Police Department
17. Northlake Police Department
18. Richardson Police Department
19. Dallas Police Department
20. Collin County Sheriff
21. Sherman Police Department
22. Denison Police Department
23. Deerpark Police Department
24. Friendswood Police Department
25. Rowlett Police Department
26. Rice Police department
27. Houston Police Department
28. El Paso Police Department
29. Kemah Police Department
30. Grayson County Sheriff
31. Plano Police Department
32. Corinth Police Department
33. Whitesboro Police Department
34. Denton Police Department
35. Galveston County Sheriff
36. Bonham Police Department
37. Paris Police Department
38. Amarillo Police Department
39. Mesquite Police Department
40. Temple Police Department

Appendix C

CYBERCRIME INVESTIGATIVE UNITS IN DEPARTMENTS



1. No Cybercrime investigative unit (63%)

2. C.I.D. Investigated Cybercrime offenses (22%)

3. Full cybercrime investigative Unit (15%)