Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future

Sameer Hinduja[1]
Florida Atlantic University

Abstract

Many traditional crimes are now being aided or abetted through the use of computers and networks, and wrongdoing previously never imagined has surfaced because of the incredible capabilities of information systems. Computer crimes are requiring law enforcement departments in general and criminal investigators in particular to tailor an increasing amount of their efforts toward successfully identifying, apprehending, and assisting in the successful prosecution of perpetrators. In the following text, key research findings in the area of traditional American criminal investigations are summarized. Similarities and differences between traditional and computer crime investigations are then presented, and consequent implications are discussed. Pragmatic suggestions as to how American computer crime investigative task forces can most competently fulfill their intended objectives are given in conclusion via a hypothetical example of a specialized unit. It is hoped that past knowledge can be assimilated with current observations of computer-related criminality to inform and guide the science of police investigations in the future.

Keywords: computer crime, investigations, police, law enforcement, internet, high-tech, justice

Introduction

Criminal investigation has been a topic of study for academics and practitioners alike, and is defined as 'the process of legally gathering evidence of a crime that has been or is being committed' (Brown, 2001:3). It seeks to identify the truths associated with how and why a crime

[1] Assistant Professor, Department of Criminology and Criminal Justice, Florida Atlantic University, 5353 Parkside Drive, Jupiter, Florida, USA Email:hinduja@fau.edu

occurred, and works toward building a case that may lead to the successful prosecution of the offender(s). Many research studies have sought to determine the best way in which the investigative process can be conducted and managed. The overarching goal of these studies has been to enable police departments to reflect upon their own practices against the backdrop of the findings, and then to implement salient positive changes which would improve the day-to-day operations of their organization. Practices of investigation have been modified and refined over the years, taking into account changes in social, political, economic, and scientific domains. These practices have infused 'science' into an activity that was once primarily considered an 'art' (Beveridge, 1957), and have consequently enhanced the investigative process.

In his law of insertion, Gabriel Tarde ([1890] 1903) asserted that novel forms of criminal behavior are fostered through the superimposing of new practices onto traditional ones, often through technological advances or innovation. Due to the exponential growth of information technology in modern society, many traditional crimes are now being aided or abetted through the use of computers and networks, and criminality heretofore never conceived has surfaced because of the incredible capabilities of information systems. These computer crimes[2] will require law enforcement departments in general and criminal investigators in particular to tailor an increasing amount of their effort towards successfully identifying, apprehending, and assisting in the successful prosecution of perpetrators.

In order to develop a sound strategy in this regard, it is crucial to learn from past research in the area of investigations, and to incorporate into law enforcement organizations those policies deemed most fruitful. In the following text, a summary of the two most important studies on traditional investigations in America is presented for the purposes of providing a historical and comparative position. Next, similarities and differences between traditional and computer crime investigations are given, and consequent implications are discussed in terms of: the role of the first-responding officer and investigator(s); information,

[2] The focus of this article is on investigations of: 1) traditional crimes in which a computer is used in an ancillary manner, and 2) nontraditional or high-tech crimes in which a computer is the primary object of, instrument in, or repository of evidence related to, a crime.

instrumentation, and interviewing; evidence collection and processing; jurisdictional issues; reactive and proactive strategies; and utility of symbolic investigations. The current work concludes with some pragmatic suggestions as to how computer crime investigative task forces should be created and managed to competently fulfill their intended objectives. This is presented via a hypothetical example of a specialized unit.

Seminal Research on Investigations

Rand study of criminal investigation

In the 1970s, the RAND Corporation in the United States (US) conducted a nationwide study of criminal investigations by law enforcement departments with over 150 sworn officers or serving a population over 100,000. Through analyses of various agencies with differing investigative philosophies, comparison with official crime statistics to determine investigative efficacy, and a review of detailed case studies, a comprehension of how agencies managed and organized investigations was sought. Four main conclusions were set forth:

1. *Case solution*: The most important determinant of case solution was the information provided to the responding officer by the victim (Greenwood, Chaiken, & Petersilia, 1977). It was also discovered that follow-up investigations were largely ineffective. Specifically, if the victim was not able to provide identifying information of the perpetrator, it was unlikely that apprehension would result. The importance of the responding officer highlighted the need for well-trained patrol personnel with a larger investigative role, who are then singularly capable of closing many cases rather than turning them over to another person (see also Block & Weidman, 1975; Greenberg, Elliot, Kraft, & Proctor, 1977). As a consequence, this would allow specialized investigative forces to address only those incidents that absolutely require expert abilities, and would keep their caseload to a manageable size.
2. *Investigative effectiveness*: Differences in investigative organization, training, staffing, workloads, and procedures did not proportionately affect crime rates, arrest rates, or clearance rates.
3. *The processing of physical evidence*: While law enforcement departments collected a great deal of physical evidence, much of it was not processed in

an effective manner. As such, the suggested policy involved the allocation of more resources to the processing of collected evidence, which would thereby have a positive impact on crime-solving.

4. *Investigative thoroughness*: Investigators were generally failing to thoroughly document all of the important evidentiary facts that would strengthen the ability of prosecutors to obtain the most appropriate convictions. Incompleteness in documentation, it was argued, may have contributed to an increase in the number of case dismissals and a weakening in the plea bargaining position of prosecutors (Greenwood et al., 1977). This deficiency in comprehensive recordkeeping necessitated immediate attention.

PERF Study on the Investigation of Burglary and Robbery

In another important study led by John Eck under the auspices of the Police Executive Research Forum (PERF), more than 3,360 burglary and 320 robbery investigations over a two-year period were analyzed in three jurisdictions: DeKalb County, Georgia; St. Petersburg, Florida; and Wichita, Kansas. The PERF study differed from the earlier research by RAND in that it focused on the entire investigative process, rather than only on the cases cleared by arrest. As such, Eck was able to determine the impact of a host of variables which affected the outcome to disproportionate degrees.

A primary finding was that both detectives and patrol officers contributed equally to the solving of cases, and that it was a disservice to emphasize one over the other (Eck, 1983). The research also found that individuals in both positions should be less reliant on information provided by the victim and more proactive in exploring leads provided by others related to the incident (Eck, 1983). The practice of neighborhood canvassing and the use of informants were asserted as important techniques to increase the effectiveness of investigations. It appeared that while most information came from the victims of the crime during the initial police response, much of those leads were unfruitful. When other sources were consulted, however, much more useful information was discovered.

The necessity of being sensitive to victims was also underscored by Eck, who asserted the relative uselessness of re-interviewing the victim during follow-up investigations. Physical evidence was found to be most useful to corroborate preexisting identifications rather than as a means to identify suspects who were previously unknown (Sanders, 1977; Wilson, 1976). Cooperation, information sharing, and information management among police departments were also extolled as key factors in successful investigations (Eck, 1983).

One of the most practical recommendations to stem from Eck's study concerned the categorization of cases into three groups – those that could be solved, those that have been solved, and those that may be solved through some effort (Brown, 2001). This 'triage system' was devised to assist law enforcement personnel in making objective decisions as to which cases were worthy of resource expenditure. Through this form of case screening, investigations could proceed in a targeted and informed manner after determining the presence of certain solvability factors that would most likely lead to a case clearance. In addition, this procedure also allowed law enforcement to tailor their efforts toward the small group of habitual offenders or 'career criminals' who commit the majority of serious crimes (Wolfgang, Figlio, & Sellin, 1972). Eck felt that these recommended changes would go a long way in refining the process and improving its utility and success rate.

From these two intensive research endeavors in the US, some important lessons can be learned. First, the role of the responding officer is crucial in investigations, and oftentimes the information provided to him or her is the deciding factor in solving a case. Additionally, it appears that expanding the breadth of investigations by exploring other avenues of information acquisition may prove valuable, as informative qualitative data can be gained in this manner. Allocating resources only to those cases most likely to be solved is another wise strategy that law enforcement departments can employ. Finally, thoroughness in evidentiary documentation is seemingly critical to building a strong case and increasing the likelihood of a successful conviction by the prosecuting team.

Definitional differences

As mentioned, investigative practices and procedures for both traditional crimes and highly developed forms of computer crime are similar in many respects simply because of a recursive process inherent in the modification of traditional crimes through innovation or technological development (Tarde, [1890] 1903). Nonetheless, vital differences exist in the investigative process, and these must be accommodated to best address computer crime. These differences are largely revealed by the definitional distinctions therein.

Traditional crimes generally concern personal or property offenses that law enforcement has continued to combat for centuries – such as the Type I offenses of the FBI's Uniform Crime Report in the US. *Nontraditional crimes*, for the purposes of the current work, encompass those involving a computer. These historically have not received a proportionate amount of attention as compared to traditional crimes, despite their gravity and the substantive harm they often cause (Braithwaite, 1985; Hinduja, 2004; Newman & Clarke, 2003; Parker, 1976; Rosoff, Pontell, & Tillman, 2002; Webster, 1980). Furthermore, they do not elicit the same visceral and emotionally-charged reaction from the American public and political system as do the conventional personal and property crimes that police largely work to address (Benson, Cullen, & Maakestad, 1990; Cullen, Link, & Polanzi, 1982). Since these entities significantly influence the policies and actions of the US criminal justice system, the result is a comparatively small amount of effort and resources allocated for computer crime.

Computer crime has been defined as 'any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime' (Royal Canadian Mounted Police, 2000). Some of the most prominent types include e-commerce fraud, child pornography trafficking, software piracy, and network security breaches. Investigative difficulties are introduced when attempting to tackle computer crime because of its generally technologically-advanced nature, the fact that it can occur almost instantaneously, and because it is extremely difficult to observe, detect, or track (Leibowitz, 1999; United Nations, 1994; Wittes, 1994). These problems are compounded by the relative anonymity afforded by the Internet as well as the transcendence of geographical and physical limitations in cyberspace, both of which render difficult the detection of criminals who are able to take advantage of a virtually limitless pool of victims.

Application and extension to computer crime

A multitude of aspects related to investigations are necessarily implicated when considering how traditional practices must be modified, augmented, or even restructured to compensate for differences inherent in computer crime. While there is no universally applicable panacea, it appears that acknowledging and accommodating the following points will result in greater investigative efficacy when addressing high-technology wrongdoing. Before proceeding, though, it must be stated that while this work specifically concentrates on investigations of computer crime, some examples of white-collar crime that can occur through the use of computer systems are presented to support the assertions.

Role of the First-Responding Officer

As previously stated, one of the most important findings of the RAND study concerned the role of patrol officers who first respond to a crime scene. It was suggested that these first responders be granted additional investigatory responsibilities to ease the caseload burdens of specialized investigators, and because their initial presence on the scene often gave them information to use as leads to explore (see e.g., Block & Weidman, 1975; Greenberg et al., 1977). By extension, the role of the first responding law enforcement officer in computer crime cases is of critical import because the evidence associated with a computer crime is often intangible in nature. Certain precautions must be taken to ensure that data stored on a system or on removable media is not modified or deleted - either intentionally or accidentally (Lyman, 2002; Parker, 1976). Even the simple shutting-down of a computer can change the last-modified or last-accessed timestamp of certain system files, which introduces questions associated with the integrity of the data. In sum, to preclude vulnerabilities in the prosecutor's case and to adequately defend against any related challenges, grave care must be exercised by first responders during the search and seizure of computer equipment.

Depicting some parallels to the subject matter at hand is the collection of hair, bodily fluids, and clothing samples from which DNA is extracted. They have no obvious use or meaning until a criminalistics expert analyzes them and consequently determines their forensic significance. Once cogent knowledge and proof is obtained from these samples by properly-trained personnel, however, the investigation and its attendant efforts towards achieving justice are often simplified. In a similar vein, specialized skills must be taught to first-responding officers who might encounter technological evidence which on the surface may appear meaningless but upon further analyses by computer forensic examiners might prove crucial in clearing a case.

Role of the Investigator

The research of Greenwood et al. (1977) stated that over 50% of traditional street crimes are solved based on information provided to the responding officer by the victim(s), and that in cases where incomplete or unusable information is provided by a victim, most are not subsequently solved through investigative efforts. Other research has likewise shown that little is gained through police effort to aid in offender apprehension following the commission of a crime (Block & Bell, 1976; Skogan & Antunes, 1979). Indeed, Skogan and Antunes (1979:223) have specifically stated that 'investigatory follow-up work, the gathering of physical evidence, and the ferreting out of criminals through detective work, play a relatively unimportant role in identifying and apprehending offenders.'

Nonetheless, the role of the investigator in computer crime cases will be much more important in clearance and arrest rates than information presented to him or her by the responding officer, victims, or witnesses. Due to the veiled nature of the techniques associated with computer crime and even the actual victimization itself, much effort will seemingly be expended in order to identify evidentiary facts, interpret clues, follow leads, and gather data to make a compelling case against the suspect(s). In addition, the PERF study recommended that officers work to locate witnesses through a neighborhood canvass; a similar procedure can be fruitful in an organizational context where computer crime has occurred. The scope of the investigation can be expanded to include interviews with other persons who might provide qualitative information related to pressures, demands, constraints, motives, and rationalizations that affect behavior. Accordingly, a sense of how the organization shapes and impels behavior may be captured, and can thereby assist the investigator in better comprehending possible stimuli for crime commission.

Information, Instrumentation, and Interviewing

O'Hara & O'Hara (1980) have written that there are three components of the criminal investigation: information, instrumentation, and interviewing. While technology and technique might change, these fundamentals persist across time and are therefore worthy of delineation. *Information* simply refers to the fact that criminal investigation is centered around the gathering, organizing, and interpreting of data directly or tangentially related to the case. Second, *instrumentation* is related to forensic science and the specific techniques afforded to crime-solving investigators. For example, technological advances such as biometrics, DNA analyses[3], and audio/video data processing will continue to enhance the accuracy of law enforcement in clearing cases. Third, *interviewing* involves the process of soliciting and lawfully extracting information from individuals who are knowledgeable about the circumstances of a crime in some capacity.

These three fundamentals have been – and will continue to be – utilized in the investigation of traditional offenses in the US in a relatively straightforward manner. However, their application to computer crime is less clear and seemingly more nuanced. Information accumulation will continue to be the 'bread-and-butter' of the investigation of these nontraditional crimes. In fact, the skill of the investigator is largely rendered irrelevant if he or she is not provided with enough useful information to move toward case clearance during the course of the investigation. Similarly, even the most adept investigator will encounter difficulties if information culled during its course is incomplete or generally inapplicable. With this in mind, though, instrumentation and interviewing – which are simply other methods to gather information – should be executed in a distinctively different manner.

Instrumentation in investigating *financially-related* crimes involving computer systems primarily revolves around the tracking and analysis of

[3] Though outside the scope of this work, it is interesting to consider how the expertise of DNA evidence collection and analyses migrated into the police organization, and whether the development of that specialized component can serve as an instructive template for the introduction and maturation of computer forensics expertise.

records and logs to determine discrepancies or irregularities in the normal order. For example, money laundering with the use of computers concerns the process of concealing the source of illegally-obtained money and often involves the creation, fabrication, or alteration of documents to create a legitimate paper trail and history (Lyman, 2002). Financial institutions are presumed to keep detailed records of all transactions, currency exchanges, and the international transportation of funds exceeding a certain amount. Additionally, the Bank Secrecy Act of 1970 requires these institutions to maintain records that 'have a high degree of usefulness in criminal, tax and regulatory investigations and proceedings' and authorizes the Treasury Department to require the reporting of suspicious financial activity which might be related to a law violation (Office of Technology Assessment, 1995).

Another example testifies to the importance of instrumentation when dealing with computer-related wrongdoing. Before the exponential growth of the Internet, the investigation of credit-card fraud often involved accurate identification by witnesses and the collection and identification of condemning physical evidence. When an offender made a purchase at a retail establishment through the use of a fraudulent credit card for payment, sales clerks and store employees trained in accurately observing and remembering physical and behavioral details of perpetrators were able to assist in the investigation. Catching an offender in possession of the fraudulently-acquired merchandise was also easier since purchases were made in a physical location. Finally, the handwriting sample obtained when the goods were signed for, and fingerprints left at the scene of the crime, also served as corroborating evidence. With the advent and growth of electronic commerce, however, the assistive role of witnesses and physical evidence – sources of information previously (and even heavily) relied upon – has now been largely eliminated. Combined with inter-jurisdictional complications, a deficiency of available investigatory resources, and the fact that these crimes occur in such an unconstrained and unregulated manner in cyberspace, the problem is further confounded. Investigators of computer crime must consequently pursue other avenues of inquiry and learn to master information retrieval from these sources, or else continue to struggle in their case clearance attempts.

The third component - interviewing - appears to be less salient as a *direct* method to investigate computer crime, largely because the victim is often unaware (either immediately or even for a great length of time) that a crime has occurred and that harm has resulted (Parker, 1976; Webster, 1980). Information useful in the solving of these cases is sometimes only identified after ferreting through reams of data on a computer system, and often the victim's only role in these investigations is to report the crime and provide access to the data storage machines. Furthermore, witnesses in computer crime are relatively rare since these offenses tend to occur behind closed doors (Rosoff et al., 2002). The only witnesses in most cases are those who commit the crimes either individually or collectively, and therefore other techniques to gather information must be utilized (Lyman, 2002).

Interviewing, then, may provide *indirect* utility for the investigator – such as insight into the motives and possibly the specific techniques employed, particularly if the offender was an 'insider.' Motive for a crime such as embezzlement (the siphoning off of funds from an employer by an employee – often through the use of computer systems (Lyman, 2002; Rosoff et al., 2002)), for example, might stem from organizational variables – such as pressure from supervisors or managers to demonstrate productivity or effectiveness, or from a 'culture of competition' that permeates the enterprise (Coleman & Ramos, 1998). It might also stem from individual-level variables such as a personality characterized by laziness, vengeful inclinations, a tendency to mock authority, or an inability to deal with stress in a pro-social manner (Krause, 2002). Coworkers of a possible suspect may provide useful secondary information in this regard, while also outlining the capabilities of (and methods potentially used by) the individual to bypass access controls to commit the crime. The task of the investigator would then be to evaluate the viability of the anecdotal feedback received, and to follow leads which may uncover stronger evidence that would hold substantive weight in a court of law.

Evidence Collection and Processing

In terms of evidentiary issues, the preliminary investigation strategies associated with computer crime should be executed as any other type of crime. Law enforcement departments have procedural requirements for evidence collection that should be followed, but certain subtleties endemic to computer crime must be noted. For example, Lyman (2002) points to the complexity associated with the lack of tangible evidence and an actual scene to be examined. As such, it is suggested that the investigator learn as much as possible about the victim and the possible suspects in a case. Though not exclusive in their impact, this highlights the salience of understanding individual-level variables as predictors of this form of criminality. Furthermore, the detailed analyses of logs, records, and documents associated with the unlawful transaction or action must occur (Lyman, 2002). The collection and use of physical evidence has been documented as vital (Eck, 1983), and while this procedure in investigating computer crime is very time-intensive, it often yields key clues that can lead to an apprehension.

The manner in which evidence is procured in computer crime cases remains a sizable challenge for law enforcement. Specific information related to the computer system requiring search and possible seizure must be detailed in the warrant in order to be approved, and also so that the prosecutor can counter any evidentiary challenges brought by the defense staff. Consistent investigative standards and protocols for computer crimes have not yet become firmly ensconced in most police departments, and this can lead to evidence being deemed inadmissible – evidence that otherwise might have led to a conviction (Lyman, 2002; Webster, 1980).

Search warrant proceedings for traditional crimes are familiar and routine to the courtroom workgroup. Due to the relative newness of search warrant applications for computer crimes, however, some states are specifically designating individual judges to deal with these specialized requests (New Jersey Attorney General Commission of Investigation, 2000). Nonetheless, requests must still be presented in a manner that allows ease of comprehension. The judge must not be confused by the technical details associated with the investigation, but should understand the nuances of what is involved so that the court can make an informed decision. The goal is to clearly articulate probable cause that a crime has been committed, and that the items described in the warrant are related to that crime. Likewise, technological jargon is often used by victims to communicate the specifics of the victimization and possible sources of investigative clues, and many law enforcement officers themselves may not be able to fully understand the information, nor assimilate it to direct or refine the investigation (Lyman, 2002). More police agencies are employing technicians who can assist responding officers or detectives in the proper preservation, collection, and processing of evidence, as well as with interpretation and presentation of the technological details of crime commission.

Once evidence associated with a computer crime is lawfully discovered, multiple safeguards should be instituted to preserve its continuity and integrity. Extreme attention must be given to the specifications on the search warrant so that all relevant items are properly and legally seized. Moreover, it is paramount to protect physical and removable media because of their sensitive nature. Magnetic fields and even static electricity have the potential to render unusable and unreadable certain electronic equipment such as data storage devices or disks. Another critical point is that suspects in a case should be restricted from the computing environment because of the possibility that digital evidence might be altered or deleted (Lyman, 2002).

At this point, the forensic analysis of computer hard drives has proven to be beneficial in building a case against a suspected criminal. This method of evidence acquisition, however, is technically complex and laborious. While the number is increasing, many law enforcement departments do not have the expertise to perform these techniques and must outsource their forensic analysis requirements to other agencies that do have skilled personnel. Unfortunately, with the continued increase of computer crime and the limited resources available for law enforcement to deal with traditional crimes - let alone novel instantiations of them - backlogs are invariably created and rows of computers often become lined up in evidence rooms awaiting analyses by a technician (Bhaskar, 2006; Bogen & Dampier, 2004; Newville, 2001). In accordance with intuition, priority is given to computer crime cases involving potential or actual physical harm to individuals. Nonetheless, backlogs invariably compromise the celerity with which justice is served to perpetrators of other offenses, and consequently undermine the viability of the system itself.

Finally, the RAND study (Greenwood et al., 1977) underscored the necessity to refine and optimize evidence processing efforts, and the PERF Study (Eck, 1983) highlighted the utility of collecting evidence to corroborate and strengthen the case against a suspected offender, rather than used to identify a suspect. These policy suggestions have been assisted and supported by recent technological advances, such as software that can analyze hundreds of gigabytes of electronic financial data for the purposes of detecting inconsistencies, and programs that can parse log files quickly to hone in on the specific activities of offenders. Unquestionably, more equipment, personnel, and training are essential to further improving the efficiency of the process.

Jurisdiction

Since national boundaries effectively disappear when considering many computer crimes, jurisdiction is another complicated matter. While a complete examination of jurisdictional issues is beyond the scope of this work, it merits comment that countries differ in civil and criminal offense standards, substantive and procedural law, data collection and preservation practices, and other evidentiary and juridical factors (Lyman, 2002). Moreover, it is often ambiguous as to whose responsibility it is to address a particular crime or spearhead an investigation, or how best to collaborate through extradition and mutual assistance policies. This plays out not only on an international level, but also within nations where multiple law enforcement departments are implicated.

Reactive and Proactive Investigations

Another distinction illumined in the literature is between reactive and proactive investigations (Lyman, 2002). Intuitively, reactive investigations attempt to solve crimes that have already occurred; this is the most frequent type. Proactive investigations attempt to deal with crime prior to the victimization, rather than after it has exacted harm on an individual, a corporation, or society. This often takes place through novel and innovative programming designed by criminal justice organizations and assisting entities, such as situational crime prevention strategies (Newman & Clarke, 2003). When law enforcement is able to anticipate the commission of certain crimes, personnel are often deployed to survey and target resources towards a known group of criminals or to counter a specific type of crime. This type of investigation is primarily intelligence-led, which underscores the importance of collecting and appropriately responding to useful data from viable sources while concurrently accounting for issues related to civil liberties and evidentiary rules.

For example, the monitoring of bulletin-boards and chat-rooms by investigators has led to the detection and apprehension of those who participate in sex crimes against children (Meehan, Manes, Davis, Hale, & Shenoi, 2001; Mitchell, Wolak, & Finkelhor, 2005; Penna, Clark, & Mohay, 2005). In addition, participants in online communities have contributed to preventing crimes by informing authorities about questionable behavior, who then are able to provide that information to investigators. For example, self-policing on Internet auction sites has led to the identification of attempted and completed sales of counterfeit and fraudulent items, and to the perpetrators of such crimes (Enos, 2000; Fusco, 1999). Partnerships in the US between the private and public sector involving the sharing of computer crime victimization data have also assisted law enforcement in its investigative endeavors.

'Symbolic' Investigations

Lastly, Brandl & Horvath (1991) discovered that the effort expended by law enforcement through investigative practices is positively related to victim satisfaction rates. That is, victims are more pleased with the police response when the department is able to demonstrate that due attention was given to the incident. This can occur through the acts of fingerprint dusting, mug shot showing, and the questioning of witnesses – which in truth are often performed to maintain a media-generated 'image' rather than to productively contribute to the investigation of a crime (Greenwood et al., 1977). This cumulatively underscores the importance of 'symbolic' investigations that serve purposes oriented more toward 'public relations' than 'crime solving' (Greenwood et al., 1977).

Extending this finding to computer crime, it appears that in order for the police to demonstrate that they are motivated and able to address these nontraditional offenses, they must respond in a similar fashion. Otherwise, individual and corporate victims will lose faith in the capacity of law enforcement to control crime, and a shaken confidence in the most prominent arm of the criminal justice system forebodes greater problems for society (Webster, 1980). Victims may also choose against reporting suspected or actual wrongdoing, and may turn to their own means of investigating and punishing transgressors - perhaps in an unlawful manner (Johnston, 1996; Silke, 2001). Trust must be developed to create and perpetuate a candid and constant line of communication between victims and law enforcement, so that each party can help the other in their collective goals of preempting and addressing computer crime.

Computer crime investigative task forces

As computer crime originating in the United States often implicates interstate and international laws, many cases fall under federal jurisdiction. Federal collaboration with local law enforcement and prosecutors to share intelligence and efforts through teamwork has demonstrated effectiveness in addressing traditional crimes involving drugs, weapons, gangs, and violence[4] (McGarrell & Schlegel, 1993; Russell-Einhorn, 2004). By extension, many scholars and practitioners have asserted the importance of forming comparable teams to combat computer crime with the hope of similar positive outcomes (see e.g., Conly & McEwen, 1990).

Research has recently been conducted to determine how such task forces might best meet the needs of law enforcement, the private sector, and societal members at large (Hinduja, 2004). The findings have provided some insight into the formation and organization of these dedicated teams. Most importantly, it appears that their investigative functions should be structured in a way that concentrates effort and attention on equipping personnel to accomplish their goals. Characteristics of three areas should distinguish a specialized computer crime task force from a traditional police unit: recruiting, mentorship, and promotion practices; training requirements; and outsourcing to the private sector. In the following text, each of these characteristics is elaborated in the context of a hypothetical computer crime unit.

Recruiting, Mentorship, and Promotion

[4] The United States Department of Justice's Weed and Seed Program and Project Safe Neighborhoods are two examples.

To begin, individuals who seek to become a part of the unit must have at least three years of experience as sworn law enforcement officers to ensure familiarity with their role as an agent of the state, as well as insight into the dynamics of the US criminal justice system. They should also be recommended by their supervising officer as highly technically-inclined and possessing character qualities essential to succeeding as an investigator - such as attention to detail, patience, excellent communication skills, and first-rate integrity. New recruits would then be charged with obtaining experience in some of the more mundane duties of the department. For example, new members of the unit would be responsible for assisting veterans with the acquisition, safeguarding, and analysis of evidence, the processing of paperwork to meet the requirements of the prosecuting team, the completion and archiving of reports for the department's data collection purposes, and the numerous telephone and face-to-face conversations related to specific incidents with victims, witnesses, and informants.

The key point is that new initiates would be specifically assigned to the tutelage and supervision of a veteran investigator who would have the responsibility to assimilate him or her into the culture of the unit and the investigation of computer crime cases in general. This 'probationary' period would last one year, after which time new members would be assigned their own cases. The investigation of crimes with comparatively little at stake - such as online credit card fraud, hate group propaganda on the Internet, the digital counterfeiting of checks or currency less than $1,000, software piracy, and minor unauthorized use of computing resources - would be relegated to these neophytes. Ensconced veterans would be in charge of crimes with more significant potential or actual repercussions - such as cyber-terrorism, child pornography and identify theft rings, network intrusions causing large-scale denial of service or data damage, hefty financial losses to a victim, and those offenses with possible organized crime ties.

Concerning promotion, one would incorporate a typical hierarchical ladder of positions through which officers would ascend incrementally after demonstrating proficiency at their current level. If an investigator shows much promise and has commendable case clearance and arrest rates with the type of crimes currently assigned, he or she will be evaluated for promotion to the next level where crimes with graver implications are addressed. With the increased responsibility will come greater autonomy and, of course, greater rewards contingent upon success at the new position. Greater autonomy will ultimately result in authorization to conduct proactive investigations to preempt the commission of computer crime before it occurs. Due to the controversial nature and human rights implications of proactive strategies, only long-term, highly-skilled veterans will be afforded this opportunity[5].

Training Requirements

During the aforementioned probationary period, new recruits will be required to attend numerous training workshops to deepen their knowledgebase with regard to crimes facilitated by a computer[6]. Technical sessions - on topics such as network protocols, operating systems, encryption schemes, and forensic analysis - will be complimented with legal sessions on topics such as the application for, and execution of, search warrants in these cases, and the importance of properly preserving and documenting evidentiary items and facts[7]. In the US, many of these training workshops are organized by federally-funded entities and are administrated to law enforcement personnel at no charge[8]. Certification exams will also be administered to recruits to ensure that they have truly learned the material taught, and can apply it to practical situations. Such intensive training is essential to equip unit investigators to excel in their positions.

Outsourcing to the Private Sector

[5] Proactive investigations introduce a host of techniques that alarm human rights activists and privacy advocates, such as wire-tapping, database mining and knowledge discovery, and grants of immunity and protection to informants. The ethical nature of these techniques will continue to warrant debate, and violations to civil rights must be precluded at all costs through policy and procedural guidelines developed by agencies for their investigators (Brown, 2001).

[6] Hinduja (2004) found through a survey of law enforcement agencies that when presented with the options for more training, personnel, or equipment, law enforcement agencies overwhelmingly declared a need for training over and above the other resource provisions.

[7] Hinduja (2004) discovered that the greatest training demands were in the areas of search and seizure training, and evidence collection and processing. This speaks to the importance of accumulating knowledge and experience related to the legal aspects of computer crime investigations over the need to acquire more technical expertise.

[8] For example, the National White Collar Crime Center holds workshops on basic and advanced data recovery analysis at locations across the country throughout the year.

The previous discussion appears to give no regard to the limited resources - time, personnel, equipment, and knowledge – with which most law enforcement departments continually struggle. Accordingly, the hypothesized computer crime unit would develop partnerships with the private sector to mitigate the relevance of initially inadequate resources. For example, it is presumed that American corporations would want to act in ways that demonstrate an investment in their local community for the purposes of maintaining and increasing consumer allegiance, and to receive tax breaks. As such, many of these companies could donate equipment to the unit in the form of hardware, software, and peripherals to meet law enforcement's needs for investigative tools. Even the time of a private sector employee might be provided *non grata* to the law enforcement agency if and when a technical or legal question arises that investigators are unable to answer, or when advice as to how to proceed in a case is required. A simple telephone call between these entities may be immeasurably beneficial to crime solution and successful prosecution.

With regard to computer crime, some might argue that the *entire* investigative process be outsourced to the business community. Historically, the privatization of investigations has assisted public law enforcement by allowing them to concentrate on other responsibilities, and has prevented their resources from being allocated in too sparse a manner to be useful. For example, Pinkerton's National Detective Agency was created in 1852 (Kuykendall, 1986; Lyman, 2002), largely stemming from vigilante forms of justice that prevailed in 18th and 19th century rural America. Vigilante justice has also reared its head in cyberspace, most prominently with the defacement of websites related to the Taliban and the governments of Afghanistan, Pakistan, and Iran following the September 11, 2001 terrorist attacks on America. Indeed, the federal government and private corporations have also engaged in 'self-help' and have launched counterattacks on computers that are used to penetrate or afflict their systems (Schwartau, 1999). A primary sentiment shared by organizations who strike back on their own terms is that law enforcement is impotent to competently respond due to limited resources and intelligence, the slow pace at which computer crime investigations tend to proceed, and the possibility that the vulnerability will become public knowledge (Schwartau, 1999).

Regardless of the effectiveness of these retributive acts, these corporations are technically engaging in criminal behavior subject to prosecution if caught. A mandate of any partnerships between law enforcement and the private sector should outline appropriate investigative and punitive responses by the latter, so that law violation does not occur in an attempt to obtain justice. With this caveat in mind, it appears a wiser solution would be to call upon American private sector organizations to partially fulfill essential duties related to criminal investigations. Their actions, in fact, may be more fruitful in facilitating an arrest or case clearance than those of the public sector agency.

To note, a host of companies have arisen – some with solely 'virtual' storefronts on the Internet - that are available for the outsourcing needs of individuals and businesses seeking services of network security development and management, hard drive forensic analyses and data recovery, and various other security-related tasks. It might be argued that these firms possess the skill sets and resources to competently assist law enforcement in their investigative duties, much like the Pinkerton Detective Agency. Due in parts to the comparatively lucrative nature of the business world, many of those who are technologically-skilled seek employment in the private, rather than the public, sector. Additionally, businesses are much more financially able to select and retain the most proficient workers. They are also in a better position to compile the resources and develop the infrastructure necessary to provide computer crime investigative services to other organizations – and, of course, to profit from it[9].

By building a solid infrastructure around the components of recruiting, mentorship, and promotion practices; training requirements; and outsourcing to the private sector, the likelihood of successful computer crime investigations are increased. In time, it is very possible that some other unexpected consequence will arise and affect either the

[9] Underscoring the utility of employing a private business to aid in a criminal investigation; a victim of auction fraud on eBay.com contracted a private business to perform a reverse cellular-telephone lookup, which resulted in the discovery of the home address of the perpetrator of the crime. After this information was retrieved, the victim then got in contact with the law enforcement department that had jurisdiction over the area in which the offender lived, and a sting was orchestrated which led to an arrest and case clearance of not only the current incident, but an impressive array of similar auction frauds by the same individual (Smith, 2002).

investigative or prosecutorial effort, and policies will have to be adapted towards closing any loopholes or vulnerabilities in the process. Structuring a department in this manner, however, appears to hold the most promise with which to assess and address computer-related criminality.

Discussion and Conclusion

Law enforcement will have to expand their investigative practices to competently respond to the problem at hand; thankfully, they are not starting from 'square-one.' A solid foundation has been laid through the years of modification and refinement of traditional investigations, and through empirical research assessing the relevance and efficacy of their techniques and procedures. While not all are equally applicable to computer crime, much insight can be gained from the past when developing sound policy to guide investigators in the future. The preceding text has summarized key points from previous research on traditional investigations in the United States, and has extrapolated and applied certain 'best practices' to computer crime investigative efforts. Suggestions as to how to suitably create and manage a specialized unit were also presented to inform American police departments called to address these crimes in their jurisdiction.

The preceding recommendations are not sizable deviations from traditional methods, but stem intuitively from principles with which law enforcement officials are currently familiar. All that is generally required is awareness of particular nuances associated with high-technology crimes to prevent investigative mistakes from invalidating the criminal justice effort. The knowledgebase associated with computer crime investigations will grow and be refined over time. Indeed, the techniques and strategies should eventually become as second-nature to investigators as are those they utilize to solve traditional forms of crime. The hope is that with additional research by academics and experience accumulated by practitioners, that time will come soon rather than later, as the significance of crimes involving computers demands it.

References

Benson, M. L., Cullen, F., & Maakestad, W. (1990). Local prosecutors and corporate crime. *Crime and Delinquency*, 36, 356-372.

Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber Katrina. *Communications of the ACM*, 49(2), 81-83.

Block, P., & Bell, J. (1976). *Managing investigations: The Rochester system*. Washington, D.C.: Police Foundation.

Block, P., & Weidman, D. (1975). *Managing criminal investigations: Perspective package*. Washington, DC: U.S. Government Printing Office.

Bogen, A. C., & Dampier, D. A. (2004). Knowledge discovery and experience modeling in computer forensics media analysis. *ACM International Conference Proceeding Series*, 90, 140-145.

Braithwaite, J. (1985). White-collar crime. *Annual Review of Sociology*, 1, 1-25.

Brandl, S. G., & Horvath, F. (1991). Crime-victim evaluation of police investigative performance. *Journal of Criminal Justice*, 19(3), 293-305.

Brown, M. F. (2001). *Criminal investigation: law and practice* (2nd ed.). Boston: Butterworth-Heinemann.

Coleman, J. W., & Ramos, L. L. (1998). Subcultures and deviant behavior in the organizational context. *Research in the Sociology of Organizations*, 15,3-34.

Conly, C. H., & McEwen, J. T. (1990). *Computer crim.* U.S. Department of Justice. National Institute of Justice.

Cullen, F., Link, B., & Polanzi, C. (1982). The seriousness of crime revisited: Have attitudes towards white-collar crime changed? *Criminology*, 20, 83-102.

Eck, J. (1983). *Solving crimes: The investigation of burglary and robbery*. Washington, DC: Police Executive Research Forum.

Enos, L. (2000). *Group takes aim at net auction pirates*. Retrieved December 28, 2002, from http://www.newsfactor.com/perl/story/6077.html

Fusco, P. (1999). *eBay confirms federal investigation*. Retrieved December 29, 2002, from http://www.internetnews.com/ec-news/article.php/4_73961

Greenberg, B., Elliot, C. V., Kraft, L. P., & Proctor, H. S. (1977). *Felony decision model: An analysis of investigative elements of information*. Washington, DC: U.S. Government Printing Office.

Greenwood, P. W., Chaiken, J., & Petersilia, J. (1977). *The criminal investigation process*. Lexington, MA: D. C. Heath and Company.

Hinduja, S. (2004). Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams. *Policing-an International Journal of Police Strategies & Management*, 27(3), 341-357.

Johnston, L. (1996). What is vigilantism? *British Journal of Criminology*, 36(2), 220-236.

Krause, M. S. (2002). *Contemporary White Collar Crime Research: A Survey of Findings Relevant to Personnel Security Research and Practice*. The Personnel Security Managers' Research Program. Aug. 2002.
Retrieved December 29, 2002, from http://www.navysecurity.navy.mil/White%20Collar%20Crime.pdf

Kuykendall, J. (1986). The municipal police detective: An historical analysis. *Criminology*, 24(1), 175-201.

Leibowitz, W. R. (1999). How law enforcement cracks cybercrimes. *New York Law Journal*, 5.

Lyman, M. D. (2002). *Criminal investigation: the art and the science* (3rd ed.). Upper Saddle River, N.J.: Prentice Hall.

McGarrell, E. F., & Schlegel, K. (1993). The implementation of federally funded multi jurisdictional task forces: Organizational structure and interagency relationships. *Journal of Criminal Justice*, 21(3), 231-244.

Meehan, A., Manes, G., Davis, L., Hale, J., & Shenoi, S. (2001). Packet Sniffing for Automated Chat Room Monitoring and Evidence Preservation. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, 285-288.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2005). Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working? *Sexual Abuse: A Journal of Research and Treatment*, 17(3), 241-267.

New Jersey Attorney General Commission of Investigation. (2000). *Computer crime: A joint report*. State of New Jersey, Commission of Investigation and the Attorney General of New Jersey. Trenton, New Jersey. Retrieved December 29, 2002, from http://www.state.nj.us/sci/pdf/computer.pdf

Newman, G., & Clarke, R. V. (2003). *Superhighway robbery: Preventing e-commerce crime*. Portland, Oregon: Willan Publishing.

Newville, L. (2001). Cybercrime and the Courts: Investigating and Supervising the Information Age Offender. *Federal Probation*, 65(2), 11-20.

Office of Technology Assessment. (1995). *Information technologies for control of money laundering*. Washington, DC: U.S. Government Printing Office.

O'Hara, C. E., & O'Hara, G. L. (1980). *Fundamentals of criminal investigation* (5th ed.). Springfield, IL: Charles C. Thomas.

Parker, D. B. (1976). *Crime by computer*. New York: Charles Scribner's Sons.

Penna, L., Clark, A., & Mohay, G. (2005). Challenges of Automating the Detection of Pedophile Activity on the Internet. *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering*, 206-222.

Rosoff, S. M., Pontell, H. M., & Tillman, R. (2002). *Profit without honor: white-collar crime and the looting of America*. Upper Saddle River, NJ: Prentice Hall.

Royal Canadian Mounted Police. (2000). *Computer crime, can it affect you?* Retrieved November 10, 1999, from http://www3.sk.sympatico.ca/rcmpccs/cpu-crim.html

Russell-Einhorn, M. L. (2004). *Federal-Local Law Enforcement Collaboration in Investigating and Prosecuting Urban Crime, 1982-1999: Drugs, Weapons, and Gangs* (No. NCJ 201782): National Institute of Justice.

Sanders, W. (1977). *Detective work*. New York: Free Press.

Schwartau, W. (1999). *Cyber-vigilantes hunt down hackers*. Retrieved December 20, 2003, from http://www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg

Silke, A. (2001). Dealing with vigilantism: Issues and lessons for the police. *Police Journal*, 74(2), 120-133.

Skogan, W. G., & Antunes, G. E. (1979). Information, apprehension, and deterrence: Exploring the limits of police productivity. *Journal of Criminal Justice*, 7, 217-241.

Tarde, G. (Ed.). ([1890] 1903). *Gabriel Tarde's laws of imitation*. New York: Henry Holt.

United Nations. (1994). *International Review of Criminal Policy - United Nations manual on the prevention and control of computer-related crime.*

Retrieved June 20, 1999, from http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html

Webster, W. H. (1980). An Examination of FBI Theory and Methodology Regarding White-Collar Crime Investigation and Prevention. *American Criminal Law Review*, 17(3), 275-286.

Wilson, J. Q. (1976). *The investigators: Managing FBI and narcotics agents*. New York: Basic Books.

Wittes, B. (1994). Perils of policing the internet: Law enforcement lacks the tools needed to go after a new breed of online criminal. The Recorder. No. October 11.

Wolfgang, M. E., Figlio, R. M., & Sellin, T. (1972). *Delinquency in a birth cohort. Chicago*: University of Chicago Press.