

COMPUTER CRIME IN NORTH CAROLINA:

Assessing the Needs of Local Law Enforcement





Written by Justin T. Davis, Research Associate

GOVERNOR'S CRIME COMMISSION

1201 Front Street, Suite 200

Raleigh, North Carolina 27609

919.733.4564

www.ncgcd.org

Graphic Design and Layout: Karen G. Jayson, Research Associate

Maps: Yuli Hsu, Research Assistant

MAY 2010

TABLE OF CONTENTS

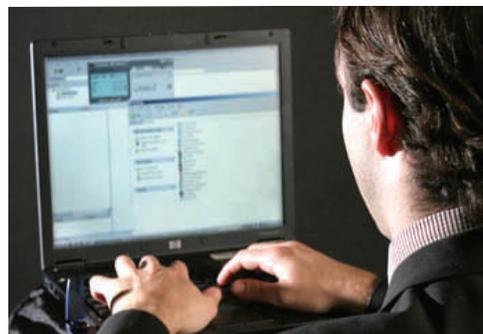
Executive Summary	1
Preface	3
Study Rationale	4
Methods	4
Results	5
Discussion	15
Appendix	18

LIST OF TABLES AND FIGURES

Table 1: Average Percent Of Cyber Case Investigations In 2008 By Responding Agencies	6
Figure 1: Law Enforcement Agencies Surveyed	5
Figure 2: Responding Law Enforcement Agencies	5
Figure 3: Degree To Which Lack of Training Impedes Investigations	7
Figure 4: Degree To Which The Inability To Monitor Internet Communications Impedes Investigations	8
Figure 5: Degree To Which Public Apathy And Lack of Awareness Impede Investigations	9
Figure 6: Degree To Which Jurisdictional Issues Impede Investigations	9
Figure 7: Degree To Which Lack of Standard Operating Procedures Impedes Investigations	10
Figure 8: Degree To Which Search Warrant Issues Impede Investigations	10
Figure 9: Degree To Which Lack of Information Sharing And Intelligence Impede Investigations	11
Figure 10: Degree To Which Lack of Technical Expertise Caused By Staff Turnover Impedes Investigations	11
Figure 11: Level of Preparedness In Regards To Investigating Cases With A Cyber Component	13
Figure 12: Average Opinions Concerning Computer-Mediated Crime	13

Executive Summary

Crimes with a cyber component once included acts such as hacking, financial fraud, theft of intellectual property and so on. Recently, crimes of this nature have evolved as citizens become more technology-savvy and gain easier access to computers. Many would agree that without proper investigative training and tools, successful prosecution of these crimes can never occur. While the primary purpose of this exploratory study is to assess investigative needs of law enforcement, the study also seeks to examine the prevalence of computer crime in North Carolina along with current procedures and activities surrounding it.



An 18-item questionnaire was developed to measure the impact of cyber crime on investigations and to determine both the strengths and weaknesses of law enforcement in dealing with crimes containing a cyber component. Part one focused on the number and types of cyber crimes experienced while part two pertained specifically to computer-mediated crime. Open-ended questions throughout the survey provided respondents with the opportunity to suggest additional training initiatives and share additional comments on what steps can be taken to lessen the extent of crimes with a cyber component.

Two distinct survey samples from police departments and sheriffs' offices were randomly selected to receive a survey by mail. Samples excluded airport, college/university, hospital and state agencies. A total of 80 surveys were distributed to sheriffs' offices and a total of 183 surveys were sent to police departments. This comprised 80 percent of all sheriffs' offices and almost 53 percent of the total number of local police departments being surveyed. The combined jurisdictional resident population of surveyed agencies comprised over 71 percent of the state's total resident population.

A total of 127 surveys were completed and returned by law enforcement agencies equating to a 48.3 percent response rate. The combined jurisdictional resident population of responding agencies comprised over 46 percent of the state's total resident population. Seventy-one counties were represented with at least one responding agency.

In 2008, responding agencies indicated that roughly 6 percent of investigations contained a cyber component. Based on a linear projection, there were approximately 26,257 cases statewide containing a cyber component in 2008. This equates to 294.1 cases per 100,000 residents, a rate which is comparable to the rate of aggravated assaults and motor vehicle thefts reported in North Carolina. The three most frequently investigated computer crimes by an average reporting agency were fraud related (79.3%), criminal threatening (8.5%), and online enticement of minors/child pornography (4.9%).

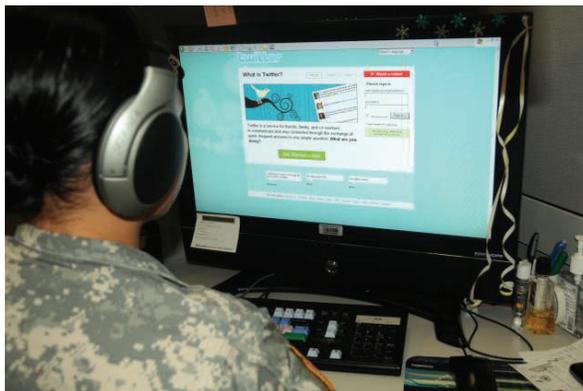


Cumulatively, respondents indicated that 198 (26.6%) of 745 investigators have received training, with the average agency reporting that one-third of their investigators had been

trained. Fifty-two percent of agencies indicated that investigators had receiving local or in-house training while 54 percent and 27 percent of agencies indicated training at the state and national levels respectively.

Over 85 percent of respondents indicated that their agencies collect computer/electronic evidence during investigation. However, only about two-thirds of these agencies reported having standard protocols established for handling evidence of this nature.

The inability to trace and monitor Internet communications and the lack of training were seen as the two largest investigative impediments for crimes with a cyber component. Another substantial concern by law enforcement is the public's apathy and lack of awareness towards crimes with a cyber component. Respondents were either indifferent or minimally concerned about the lack of standard operating procedures, search warrant issues, jurisdictional issues, lack of information sharing, and lack of technical expertise due to staff turnover.



At the time of survey, roughly four out of every 10 agencies actually conducted cyber crime prevention or awareness activities and just over 30 percent were involved in official partnerships with other agencies or private entities to combat cyber crime.

Over two-thirds of agencies expressed that they were either totally unprepared or somewhat unprepared in terms of equipment. Similarly, over half of respondents felt unprepared in terms of training and about 60 percent believed they were unprepared in terms of personnel. Law enforcement responded more positively in regards to their coordination with other agencies. Although over one-third of agencies answered neutrally, almost 39 percent of agencies believed they were prepared.

Computer-mediated crime was briefly examined as it is one of the newest types of crime involving computers and is likely to expand in coming years. For the purposes of this study, computer-mediated crimes are defined as those traditional types of crime (theft, robbery, rape, assault, etc.) that are furthered either by the use of a computer or electronic device. Many cases were mediated through means of the Internet with crimes ranging from robberies facilitated by Craigslist to statutory rape through meeting over MySpace to burglaries perpetrated after taking virtual tours of rental properties.



As a whole, law enforcement slightly agreed that they lack the power to prevent or curtail computer-mediated crime. In fact, half of respondents agreed that they have little power to curtail these types of crime in comparison to only under one-fourth of agencies who disagreed. A much higher level of agreement was measured regarding the expected growth of computer-mediated crime. Overwhelmingly, agencies agreed that their jurisdiction will experience an increase in computer-mediated crime in the next five years. One-half of

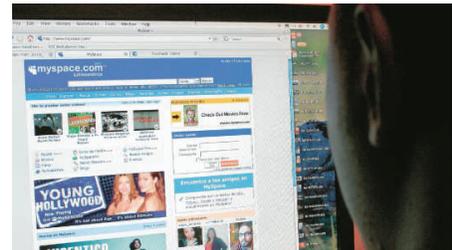
respondents agreed coupled with an additional one-third who strongly agreed that legislators should enhance penalties for traditional crimes mediated by a computer or electronic device. When surveyed about the adequacy of current North Carolina statutes for prosecuting cyber crime perpetrators, law enforcement responses were most commonly neutral. However, interestingly enough, no respondents strongly agreed and only 19 percent of respondents agreed that current statutes are adequate enough. Lastly, the survey measured opinions on whether introduction of a bill was needed in North Carolina to impede computer-related victimization. New Jersey State Legislative Bill A2864/S1429 makes it a crime of the third degree if a person attempts, via electronic or any other means, to lure or entice a person into a motor vehicle, structure or isolated area, or to meet or appear at any place, with a purpose to commit a criminal offense with or against the person lured or enticed or against any other person. Over 87 percent of respondents believed introduction of a similar bill is needed in North Carolina.



Study findings revealed several areas of concern related to the investigation of computer-related crime. According to remarks, it appears investigators and prosecutors are disconnected when dealing with crimes involving a cyber component. Funding consideration should be given to establish pilot sites for joint training sessions between detectives and prosecutors among neighboring judicial districts across the state. In addition, equipment, training and personnel must all be enhanced in hopes of curtailing cyber crimes including computer-mediated crimes.

Preface

Undoubtedly, computer technology, especially the Internet, has quickly changed daily lives in the early 21st century. The Internet has created a new way of interaction between people and has caused an online anonymity effect. For instance, without acknowledgement, everyday millions of social networking users share with the rest of the world what may seem like harmless bits of their identity such as birth date, address, school, and family member names. Furthermore, we invite complete strangers to our residences to pick up items listed on outlets such as Craigslist.



In 2004, Dr. John Suler¹ described that users of the Internet often experience an *online disinhibition effect*. He cautions this effect can work in seemingly opposite directions though. For instance, through *benign disinhibition*, individuals share personal information and often go out of their way to assist others. In contrast, through *toxic disinhibition*, people act very differently than they would otherwise act in real world situations. They may use rude language, threaten others, or even visit areas of the Internet filled with such things as crime and violence. Combinations of these effects are believed to shape online interactions and quite possibly have a significant effect on whether computer-related crimes ever occur.

¹ Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, 7(3), 321-326.

Study Rationale

Computer crimes have greatly evolved and continue to grow as the result of citizens becoming more technology-savvy and gaining increasingly easier access to computers. Crimes with a cyber component once included acts such as hacking, financial fraud, theft of intellectual property and so on. In 2003, a needs assessment on prosecuting computer crimes was conducted by the Governor's Crime Commission's Criminal Justice Analysis Center². While examining the needs of prosecutors was certainly important, it is probably even more important to take a current look at the investigative needs of law enforcement. Without proper investigative training and tools, successful prosecution cannot occur. While the primary purpose of this exploratory study is to assess investigative needs of law enforcement, the study also seeks to examine the prevalence of computer crime in North Carolina along with current procedures and activities surrounding it.

Additionally, the North Carolina Criminal Justice Analysis Center seeks to provide brief insight into an overlooked area of computer crimes -- computer-mediated crimes. For the purposes of this study, computer-mediated crimes are defined as those traditional types of crime (theft, robbery, rape, assault, etc.) that are furthered either by the use of a computer or electronic device. Recently computer-mediated crimes have included recent Craigslist killings in Massachusetts and Washington; an alleged North Carolina man eliciting someone to rape his wife through an online ad; and an alleged incident involving the burglary of an Arizona home because the home owner documented his European vacation on Twitter. Computer-mediated crimes can be something as simple as a person replying to an on-line listing of a refrigerator for sale where the perpetrator uses the opportunity in the seller's home to case the residence for a future burglary, rape, assault or other offense. In essence, computer-mediated crimes are the result of perpetrators simply using the computer as a tool to lure victims into a false sense of familiarity or safety.



Computer-mediated crimes can be something as simple as a person replying to an on-line listing of a refrigerator for sale where the perpetrator uses the opportunity in the seller's home to case the residence for a future burglary, rape, assault or other offense. In essence, computer-mediated crimes are the result of perpetrators simply using the computer as a tool to lure victims into a false sense of familiarity or safety.

Methods

Survey Instrument

An 18-item questionnaire was developed to measure the impact of cyber crime on investigations and to determine both the strengths and weaknesses of law enforcement in dealing with crimes containing a cyber component. Part one focused on the number and types of cyber crimes experienced. Questions also dealt with law enforcement's preparation in terms of training, personnel, equipment, and procedures. Respondents were asked to indicate to what degree certain issues impeded the investigation of crimes with a cyber component. The final part of the survey pertained specifically to computer-mediated crime. Questions sought to examine the extent of investigating these crimes along with the opinions on combating the problem. Open-ended questions throughout the survey provided respondents with the opportunity to suggest additional training initiatives and share any additional comments on what steps can be taken to lessen the extent of crimes with a cyber component.

² Yearwood, D. & Hayes, R. (2003) Prosecuting computer crime in North Carolina: Assessing the needs of the state's district attorneys. Raleigh, N.C.: Governor's Crime Commission.

Study Sample

A list of the number of North Carolina's law enforcement personnel by agency was provided by the State Bureau of Investigation Crime Reporting Section and was used as a basis for selecting two distinct survey samples from police departments and sheriffs' offices. Samples excluded airport, college/university, hospital and state agencies. Both sheriffs' offices and police departments were divided into four groups, or quartiles, based upon the median number of sworn personnel. A proportionate number of agencies, relative to the percent of agencies in each of the four groups, were sampled and selected to receive a survey by mail.

Figure 1: Law Enforcement Agencies Surveyed

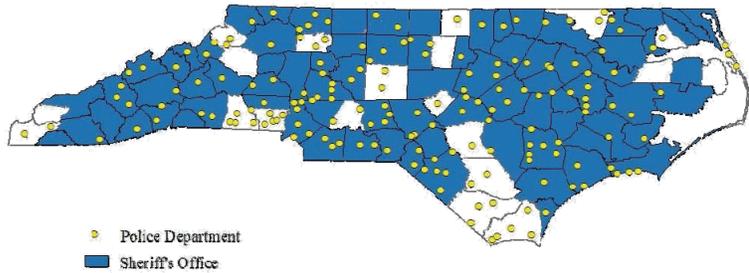
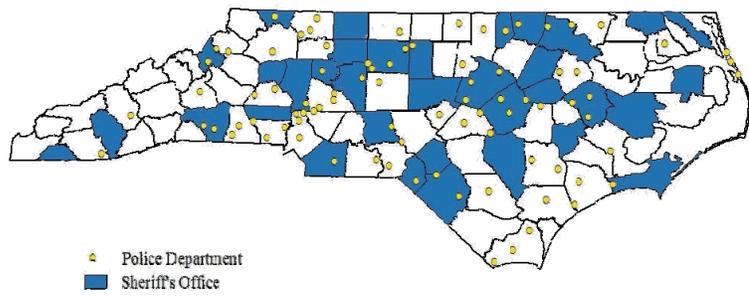


Figure 2: Responding Law Enforcement Agencies



A total of 80 surveys were distributed to sheriffs' offices with 20 (25%) mailed to agencies with more than 99 sworn personnel, 19 (23.75%) to agencies with 53 to 99 sworn personnel, and 21 (26.25%) to agencies with 29 to 52 sworn personnel. The remaining 20 surveys (25%) were sent to the state's smallest sheriffs' offices, defined as having fewer than 29 sworn personnel.

A total of 183 surveys were mailed to police departments with 46 (25.14%) sent to agencies with more than 24 sworn personnel, 42 (22.95%) to agencies with 12 to 24 sworn personnel, 42 (22.95%) to agencies with six to 11 sworn personnel, and 53 (28.96%) sent to those agencies with less than six sworn personnel.

Eighty percent of sheriffs' offices and almost 53 percent of local police departments were surveyed. The combined jurisdictional resident population of surveyed agencies comprised over 71 percent of the state's total resident population. For a map detailing the location of surveyed agencies, see Figure 1.

Results

A total of 127 surveys were completed and returned by law enforcement agencies equating to a 48.3 percent response rate. The combined jurisdictional resident population of responding agencies comprised over 46 percent of the state's total resident population. Seventy-one counties were represented with at least one responding agency. Figure 2 illustrates the location of responding agencies.

In the beginning of the survey, agencies were asked to provide the number of total investigations conducted in calendar year 2008, in addition to the number of investigations containing a cyber component and the percentage in which the cyber component was included as part of the charges. Responding agencies reported conducting a total of 264,702 total investigations, 42

percent of which were actual counts with the remaining 58 percent being estimates. As imagined, the number of investigations per agency varies greatly throughout the state (mean=2,282 investigations, median=922, mode=50). Of all investigations, respondents cumulatively indicated that roughly 6 percent contained a cyber component. However, of those cases containing a cyber component, only 12 percent actually included the cyber component as part of the prosecution's charges.

Because available and reliable data are meager at best, statewide estimates are difficult to arrive at with great certainty. Therefore, estimates should be taken with caution. An extrapolation of cases based on a linear projection, would suggest that there were approximately 26,257 cases statewide in 2008 containing a cyber component. This equates to 294.1 cases per 100,000 residents, comparable to the rate of aggravated assaults and motor vehicle thefts reported last year in North Carolina.

Each agency was then asked to approximate the percentage of cases with a cyber component into provided categories. As Table 1 illustrates, the most frequently investigated computer crimes by an average reporting agency were fraud related (79.3%), criminal threatening (8.5%), and online enticement of minors/child pornography (4.9%).

Table 1: Average Percent of Cyber Case Investigations in 2008 by Responding Agencies

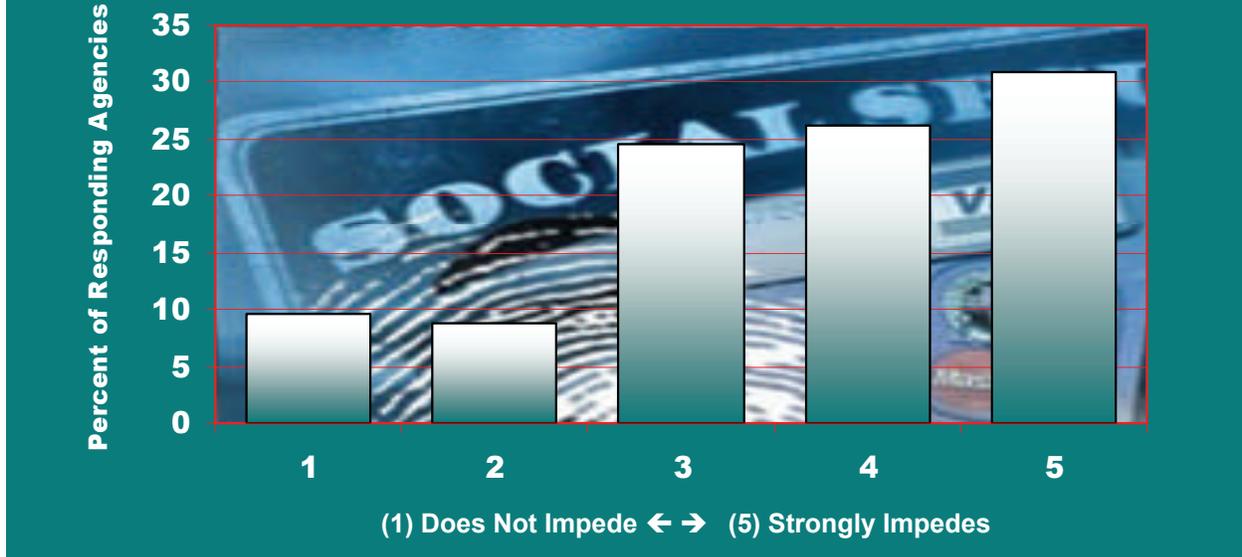
Offense	Percent
Fraud (auction, investment, credit/debit card, etc.)/ Forgery (currency, check, identification, etc.)/ Larceny (theft of physical goods, intellectual property, telecommunications services, etc.)	79.3%
Criminal threatening (cyber bullying, stalking, harassment, etc.)	8.5%
Online enticement of minors/child pornography	4.9%
Cyber attacks (intrusions, hacking, unauthorized access, etc.)/ Cyber squatting (registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else)	1.9%
Other	1.8%
Violent crimes (assault, murder, rape, robbery, etc.)	1.3%
Drug related (possession, trafficking, etc.)	1.0%

[^] Due to survey responses being provided in percentages and rounding, percentages do not total 100%.

Next, agencies were asked about the training received by investigators to investigate crimes with a cyber component. Overall, 198 (26.6%) of 745 investigators have received training, with the average agency reporting that one-third of their investigators had been trained. Fifty-two percent of agencies indicated that investigators had receiving local or in-house training while 54 percent and 27 percent of agencies indicated training at state and national levels respectively.

³ According to the State Bureau of Investigation, there were 284.3 aggravated assaults and 294.1 motor vehicle thefts per 100,000 residents in 2008.

Figure 3: Degree to Which Lack of Training Impedes Investigation



Survey recipients were questioned about the collection of evidence during investigations. Of responding agencies, over 85 percent indicated that their agencies collect computer/electronic evidence during investigation. Surprisingly, only about two-thirds of agencies reported having standard protocols established for the handling of computer/electronic data.

Respondents were asked to rate to what degree eight distinct issues impeded the investigation of crimes with a cyber component. Responses were scored on a scale of one (does not impede) through five (strongly impedes). Issues encompassed factors such as training, jurisdictional issues, and staff turnover. In terms of training, the majority (57.2%) of agencies felt that the lack of training impeded their ability to investigate crimes with a cyber component. Based on an overall average response of 3.6, there appears to be significant deficiency in this area. In fact, lack of training was recognized as the second most concerning issue that hampers investigations. As seen in Figure 3, the most common response was “strongly impedes”.

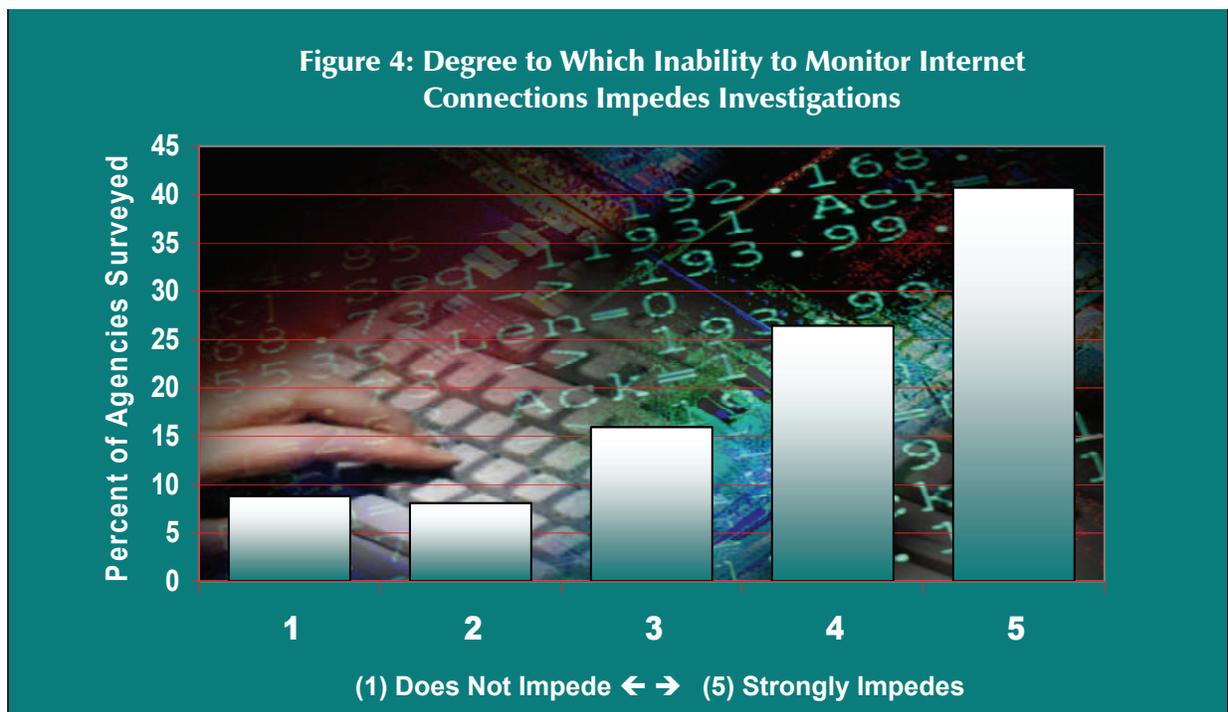
Respondents identified the following types of training not currently offered that would significantly increase their ability to investigate crimes with a cyber component:

- ◆ Basic cyber crime investigation course offered on-line
- ◆ Stalking and stalking behavior
- ◆ Computer forensics
- ◆ Cell phone forensics
- ◆ Search warrant preparation and legal aspects of cyber crime
- ◆ Network Intrusion
- ◆ Advanced Computer Forensics
- ◆ Online predator training
- ◆ IP tracking

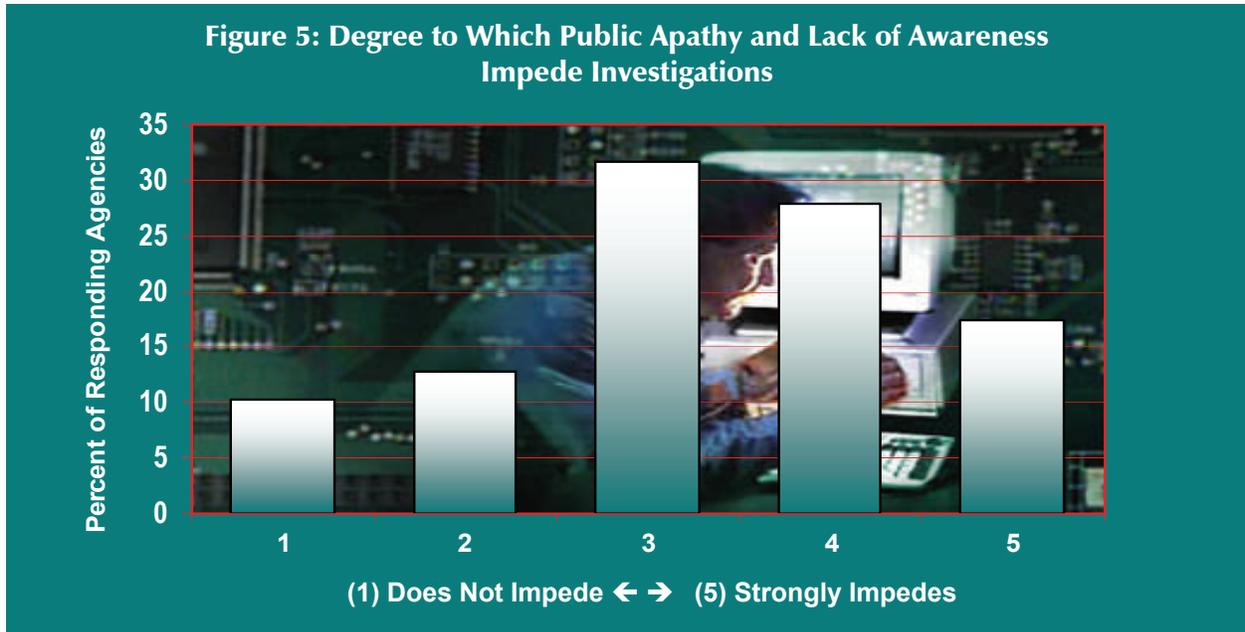
Additionally, several respondents mentioned their concerns about the overall need for training:

- ◆ “Training on specific forensic software such as EnCase and Forensic Toolkit is needed. For example, four-day training costs law enforcement agencies around \$2,000 per person alone.”
- ◆ “Training that explains the differences on uses of subpoenas, court orders, and search warrants in dealing with computer crimes.”
- ◆ “Any training in our county would be greatly appreciated.”
- ◆ “Make recruit level officers aware of computer/digital evidence and that it could be present in any type of crime. This could be accomplished in the Criminal Investigations block of instruction during Basic Law Enforcement Training (BLET).”
- ◆ “Some training is advertised, but officers are never required to attend the training.”
- ◆ “More slots are needed for classes pertaining to cyber crime. There are just not enough slots available at the Justice Academy [both at Edneyville and Salemburg].”
- ◆ “Not sure what training is offered to begin with.”
- ◆ “Training is needed for crimes in which the victim (buyer) is in North Carolina and the perpetrator (seller) is out-of-state [and never sends the item].”
- ◆ “We would like to see the training currently available closer to our area. Currently, the closest training is almost two hours away.”
- ◆ “I would like to see an increase in locally available training.”

According to law enforcement, the inability to trace and monitor Internet communications was seen as the largest impediment to the investigation of crimes with a cyber component. The average responding agency’s response equaled 3.82. Figure 4 depicts that over two-thirds felt this issue hindered their agency.



When questioned about the potential impediment of public apathy and lack of awareness, just under one-third (31.7%) of agencies were neutral on the issue. However, as seen in Figure 5, almost twice as many agencies felt public apathy and lack of awareness were significant impediments (45.3%) compared to those that did not (23%). The average response was 3.29.



In terms of jurisdictional issues impeding the investigation of crimes with a cyber component, the mean response was 3.11. Roughly one quarter (24.6%) of responding agencies were neutral while almost 40 percent of respondents felt jurisdictional issues were impediments. The remaining (35.7%) agencies expressed minimal concern. Figure 6 outlines the response in further detail.

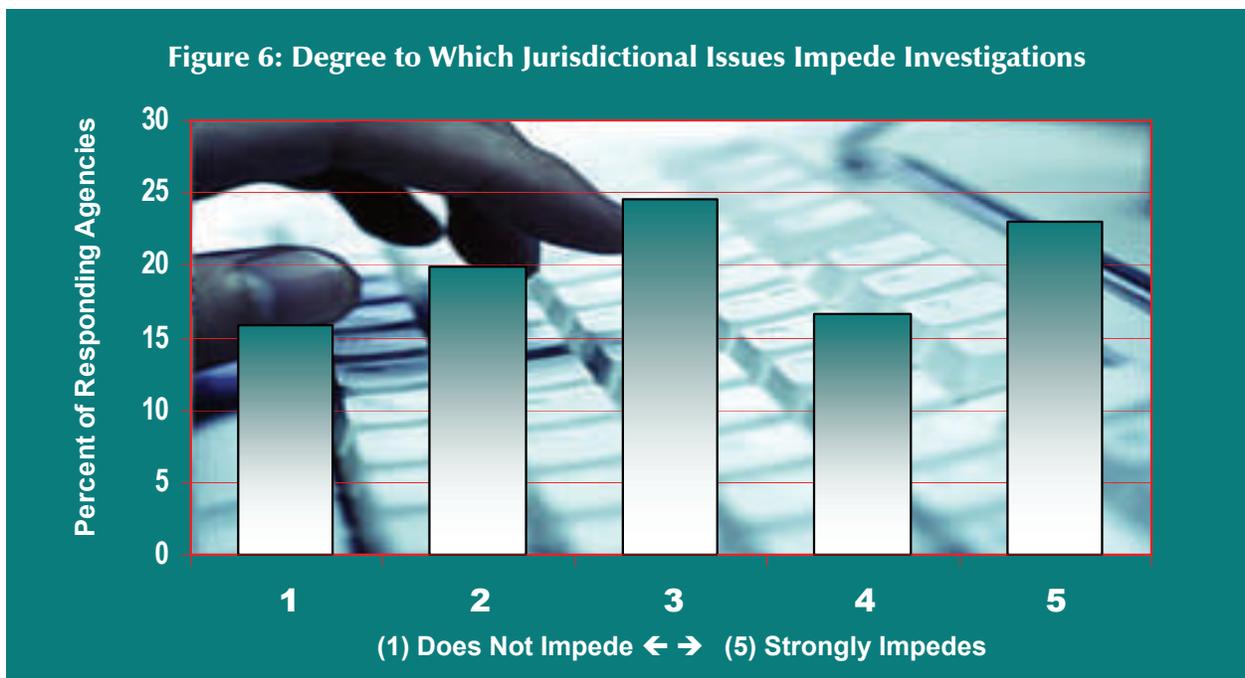
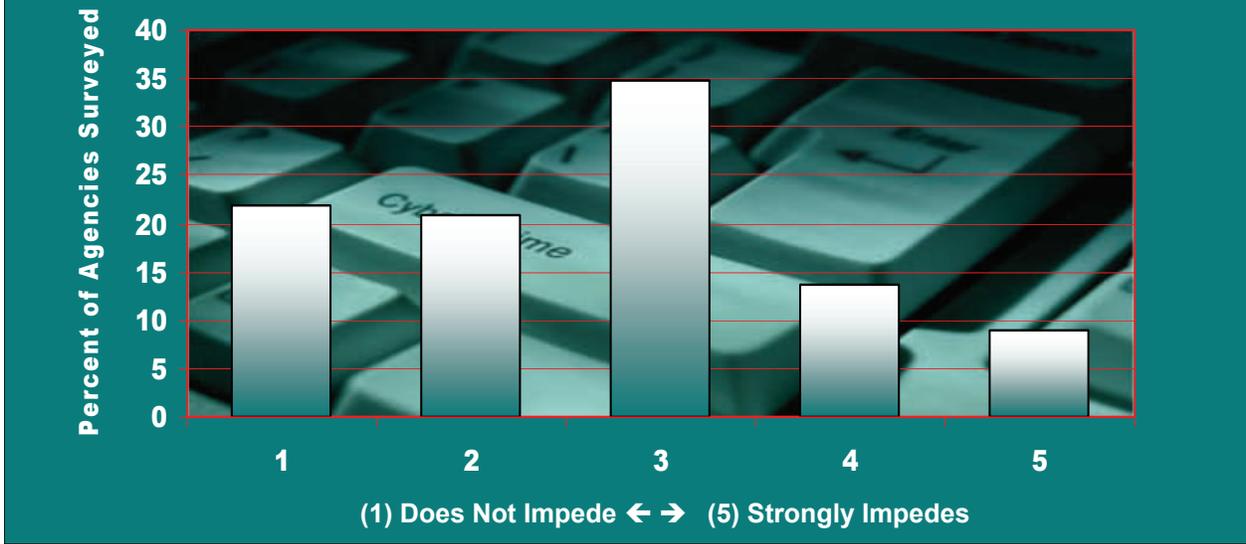


Figure 7: Degree to Which Lack of Standard Operating Procedures Impede Investigations



According to Figure 7, over three-fourths (77.4%) of respondents indicated minimal concern regarding the lack of standard operating procedures as an investigative impediment. The remaining (22.6%) respondents felt otherwise. The mean score for this issue was quite low at 2.67. Similarly, agencies felt search warrant issues had minimal impact as seen in Figure 8. Only 19 percent of agencies indicated substantial concern in this area. In fact over 29 percent of agencies responded that search warrants did not impede their investigations while the remaining (51.6%) agencies felt minimal impact. With the lowest average response of 2.41, this area was seen as the least impeding area among the eight areas.

Figure 8: Degree to Which Search Warrant Issues Impede Investigations

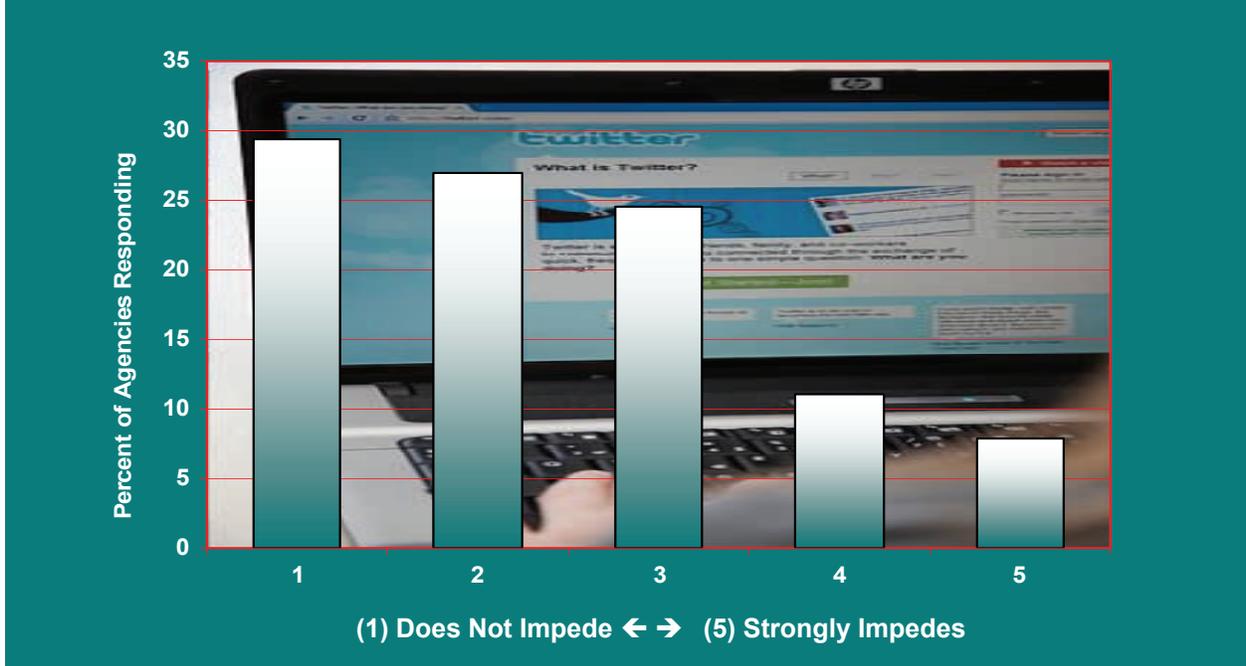
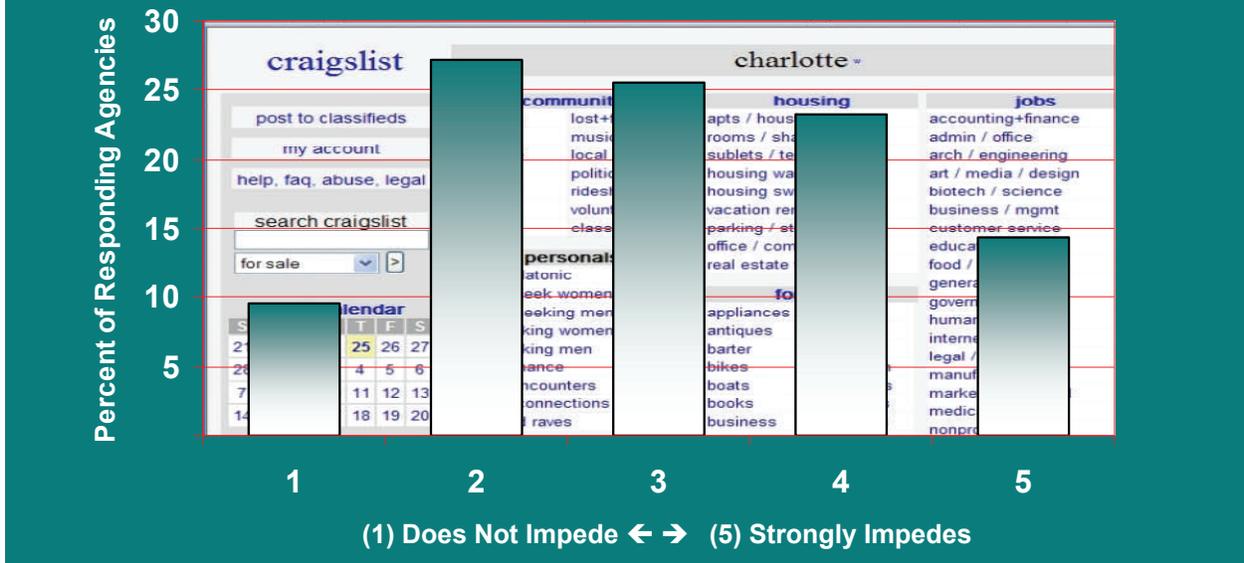


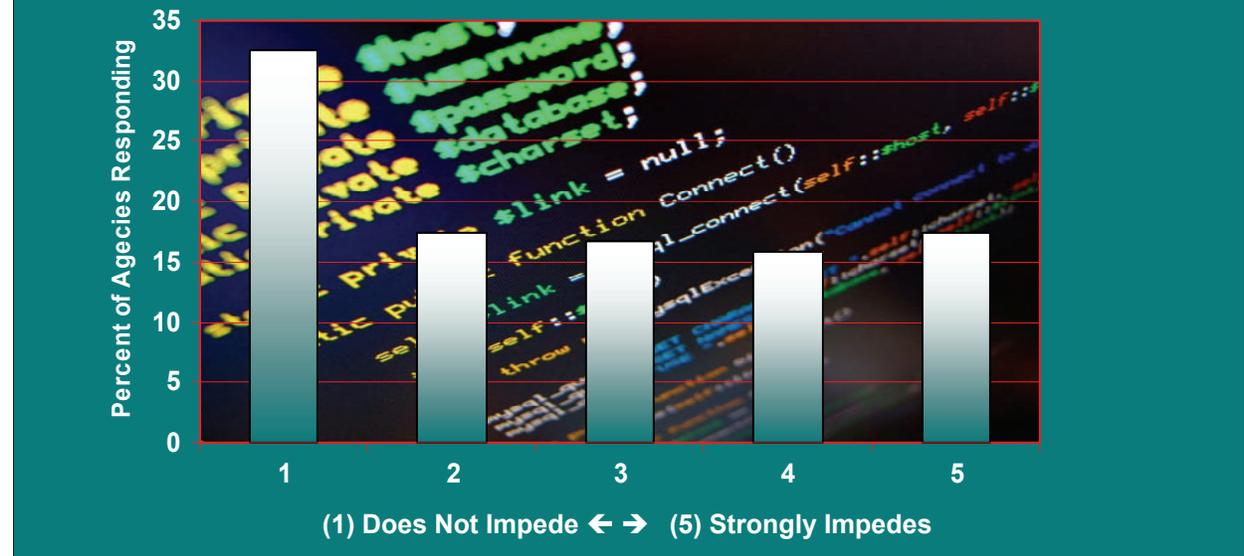
Figure 9: Degree to Which Lack of Information Sharing and Intelligence Impede Investigations



As seen in Figure 9, few (9.6%) respondents felt that the lack of information and intelligence sharing did not impede investigations. On the other hand, a relatively small percentage (14.4%) of agencies thought this particular area hindered investigations extremely. The remaining 76 percent of responses were distributed equally among the remaining three levels. With a 3.06 mean score in this category, law enforcement response can be simply described as neutral.

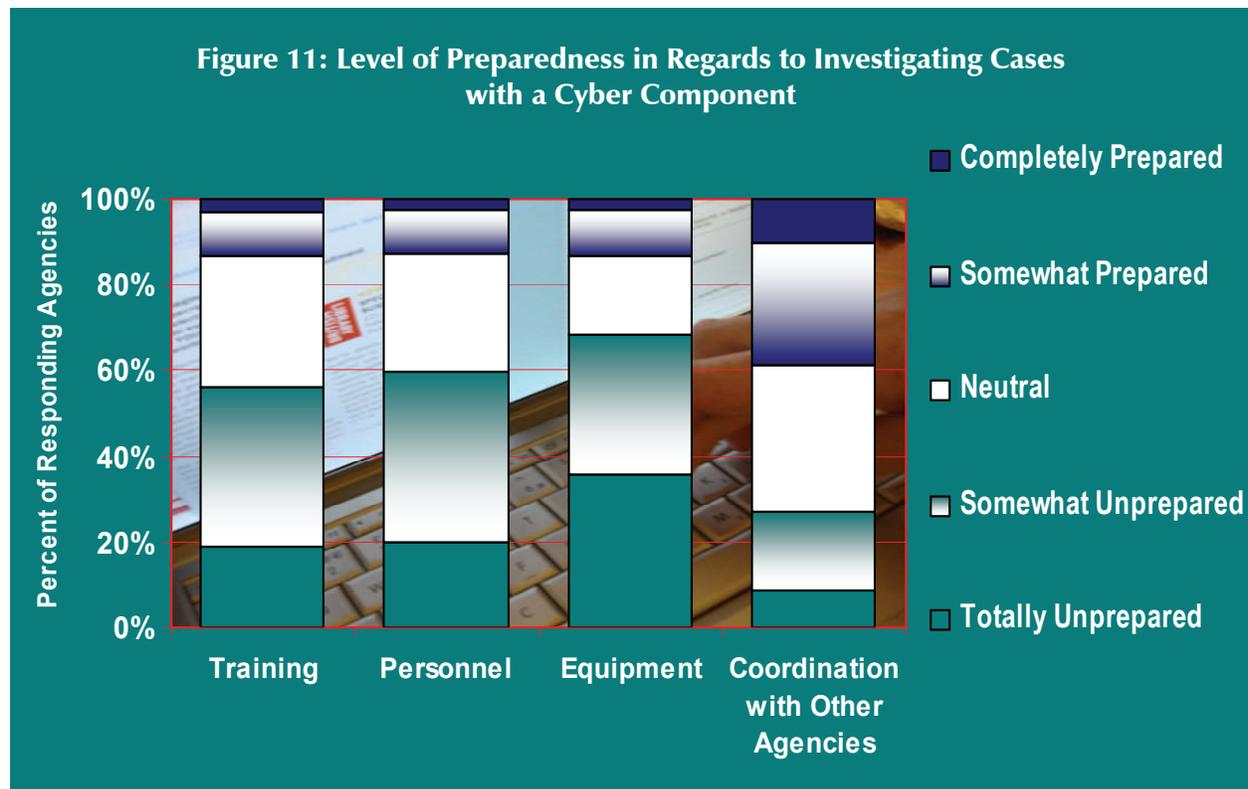
The lack of technical expertise due to staff turnover did not seem to greatly hinder agencies either, according to Figure 10. The most common response of “does not impede” accounted for almost one-third of respondents (32.5%). Responses varied the least in comparison to all other impediment types.

Figure 10: Degree to Which Lack of Technical Expertise Caused by Staff Turnover Impede Investigations



As indicated, roughly four out of 10 (41.3%) agencies actually conducted cyber crime prevention or awareness activities and just over 30 percent were involved in any official partnerships with other agencies or private entities to combat cyber crime. Agencies identified various methods of priority outreach including Internet safety for children, public information sessions on identity theft protection and online fraud prevention, and public education through newspaper articles.

Next, the survey asked agencies about their level of preparedness in certain areas regarding the investigation of cases with a cyber component. Responses were measured on a Likert scale from one (totally unprepared) to five (completely prepared). Figure 11 displays the varying levels of preparedness across four areas.

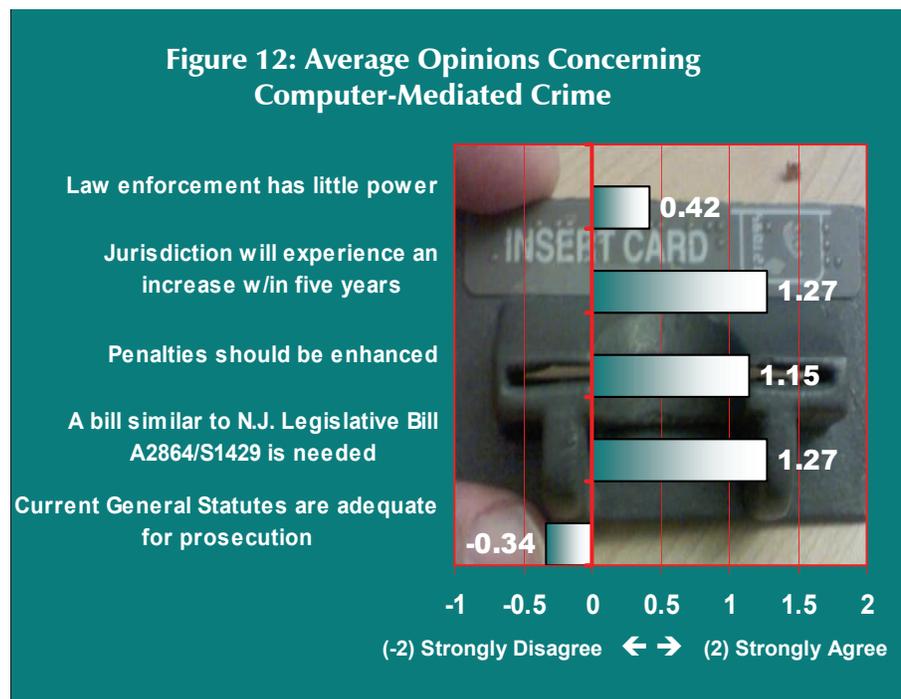


Law enforcement indicated that they were least prepared in the area of equipment with the lowest mean score of 2.12. Of those responding, over one-third (35.7%) expressed their agency was either totally unprepared in this area and roughly another one-third (32.5%) of agencies were somewhat unprepared. Although over 18 percent of respondents responded neutrally, only 13 percent of agencies felt prepared at all in terms of equipment. Agency responses in the areas of training and personnel were almost identical. Well over half (56.3%) of respondents felt unprepared in terms of training while over 13 percent indicated some level of preparation. In comparison, about 60 percent of agencies believed they were unprepared in terms of personnel, whereas close to 13 percent felt prepared. For both areas, approximately three out of every 10 agencies provided neutral responses. Fortunately, when compared to the three previous areas, law enforcement responded more positively in regards to their coordination with other agencies. Although over one-third (34.1%) of agencies were neutral, almost 39 percent of agencies believed they were prepared in this area. The remaining 27 percent felt unprepared to some degree with one in three agencies within this group feeling totally unprepared. Agencies indicated the most preparedness in this area with the highest mean score of 3.13.

The survey explored whether agencies had investigated cases in which a computer or electronic device mediated a traditional crime. Computer-mediated crime was examined as it is one of the newest types of crime involving computers and is likely to expand in coming years. Less than half (43.3%) of responding agencies had any prior experience in this area. A large portion of cases were mediated through means of the Internet. Examples of computer-mediated crimes investigated by North Carolina agencies include:

- ◆ A perpetrator planning a burglary by using a computer to draw up a plan that was used to commit the crime
- ◆ An out-of-state stalker coming to North Carolina to attempt to get a minor to leave with him
- ◆ Fraud-related crimes involving eBay where sellers advertise items but do not deliver the products to buyers
- ◆ A perpetrator using realtor virtual tours to case rental properties before committing burglaries
- ◆ A computer used to produce counterfeit documents
- ◆ Sale of stolen property through online advertisement sites
- ◆ A female's name was placed on-line advertising sexual favors as a business without her knowledge
- ◆ Prostitution cases in which females were advertising on Craigslist
- ◆ Rape cases facilitated by the meeting of individuals on MySpace
- ◆ A suspect using a computer to communicate with others about drug transactions

In the final part of the instrument, levels of agreement on five statements about computer-mediated crime were measured on a five-point Likert scale. In the analysis, levels of agreement ranged from strongly disagree, coded as -2, to strongly agree, coded as 2. Figure 12 clearly indicates that with a mean score of 0.42, law enforcement as a whole slightly agree that they lack the power to prevent or curtail computer-mediated crime. In fact, over one-half (50.4%) of



agencies agree that they have little power to curtail these types of crime while just under one-fourth (23.2%) of agencies disagree. A much higher level of agreement was measured when questioned about expected growth of computer-mediated crime. Agencies tended to agree (mean = 1.27) that their jurisdiction will experience an increase in computer-mediated crime in the next five years. With almost 85 percent of respondents agreeing that there will be an increase in coming years, more emphasis on preparedness needs to occur sooner rather than later.

The remaining three statements focused particularly on legislative issues. Respondents were asked whether penalties should be enhanced for traditional crimes mediated by a computer or electronic device. In other words, should the use of an on-line advertising site to facilitate a robbery be considered an aggravating factor at time of sentencing? Agencies indicated (mean = 1.15) that enhancing penalties in this manner should receive consideration with one-half of respondents agreeing and an additional one-third (36.3%) strongly agreeing. When surveyed about the adequacy of current North Carolina statutes for prosecuting cyber crime perpetrators, law enforcement responses were most commonly neutral (39.2%). Only 19 percent of respondents agreed that current statutes were adequate, interestingly enough none of them strongly agreed. Contrarily, roughly 41 percent of respondents did not believe statutes were adequate enough in terms of prosecution. Lastly, the survey measured the opinions on whether introduction of a bill was needed in North Carolina to impede computer-related victimization. During the 2004-2005 New Jersey State Legislative Session, Legislative Bill A2864/S1429 was introduced and passed. The bill makes it a crime of the third degree if a person attempts, via electronic or any other means, to lure or entice a person into a motor vehicle, structure or isolated area, or to meet or appear at any place, with a purpose to commit a criminal offense with or against the person lured or enticed or against any other person. Over 87 percent of survey respondents believed introduction of a similar bill is needed in North Carolina whereas 4 percent disagreed and fewer than 9 percent were neutral.



Survey recipients were asked to identify steps that policymakers or the Governor's Crime Commission could take to lessen the extent of crimes with a cyber component. A number of significant suggestions were made:

- ◆ "District attorneys and judges need to be trained and educated in electronic crimes. Most are afraid to take on these cases due to the uncertainty surrounding retrievable evidence and the technological nature of these crimes in general. It would be nice to see ADAs become trained on the technical aspects and assigned to work directly with forensic units similar to how it's done in Greensboro. Because of the partnerships they have over there, they get more convictions."
- ◆ "Policymakers should solicit recommendations from prosecutors and law enforcement as statutory changes are needed. Current legislation presents many challenges to the prosecution and does not keep up with the evolution of technology."
- ◆ "Records Management Systems, for instance Sungard's OSSI, need improvement in the way data are captured. Our numbers are conservative estimates due to not all computer

crimes being captured from field reports. When suspect information is unknown, there is no way to flag the case as one characterized by computer involvement.”

- ◆ “Regional technology investigative units would be a big help. That is, departments sharing resources and jurisdictions to fight cyber crime. This would make investigating easier, broaden the knowledge base, and would spread the financial burden out to multiple agencies.”
- ◆ “Law enforcement needs easier access to information and better tools to conduct investigations. The process for tracing IP addresses needs simplifying as it requires a lot of effort to obtain information from Internet Service Providers (ISPs).”
- ◆ “Currently, companies [ISPs] won’t release information without a subpoena.”
- ◆ “With the advance in cell phone access to the Internet, more training is needed for district attorneys and assistant district attorneys in order to ensure adequate prosecution of these types of offenses.”
- ◆ “Publish any grants that are available for local agencies to acquire computer investigative equipment (e.g., hard drive imager). Also, offer public education sessions on the topic of computer-related crime.”
- ◆ “Crimes of this nature are hard to track. We just don’t have enough resources to investigate these crimes. Thankfully, we’ve had the support of the SBI and Sheriff’s Office. Jurisdiction of these crimes needs to be clearly defined when investigating cases. In terms of equipment, some agencies need things that will help them to initially begin investigations. Currently, training offered is not geared towards your normal day-to-day officer.”
- ◆ “Ensure each agency has or has access to equipment.”
- ◆ “Smaller police agencies such as ours do not have the time or resources.”
- ◆ “There remains a strong need for assistance with funding for new computer equipment and training.”

Discussion

Current study findings reveal several areas of concern related to the investigation of computer-related crime. Oddly enough, areas closely mirror the identified areas from the Analysis Center’s needs assessment of prosecutors from almost seven years ago. That study included four recommendations pertaining to training, equipment, legislation, and case management system statistics. Among recommendations it suggested that in-state computer crime training needed to be ramped up and encouraged attendance at national training courses. Next, the study suggested prosecutors work closely with the Governor’s Crime Commission to obtain the latest information on available funding sources to address



equipment needs associated with computer crime. Third, it was recommended that current general statutes pertaining to computer crime be reviewed in addition to the range of sanctions prescribed. Finally, the previous study advised offices to improve or expand their case management systems as the ability to extract case statistics on computer-related crime would prove beneficial in measuring the impact of these crimes on overall workload.



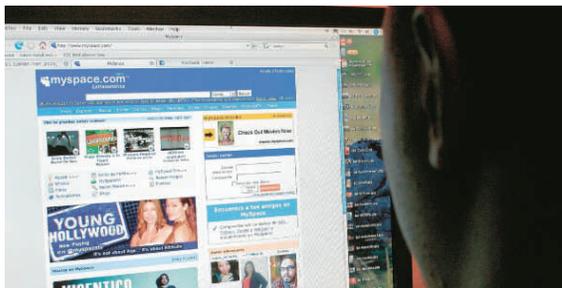
Computer-related crime is merely a part of traditional crime, however the challenges remain the same – how do we ensure the best investigation and prosecution of crime can occur and how do we educate the public to take precautionary action to protect themselves? Even though the past study explored the needs from a prosecution angle while the current one examined them from an investigation aspect, areas of concern remained practically unchanged. Clearly, equipment, training and personnel must all be improved upon in hopes of curtailing cyber crimes which including computer-mediated crimes. In summary, based on law enforcement responses:

- 1) Agencies are least prepared in terms of equipment.
- 2) There are substantial deficiencies in training and much concern over the shortage of manpower that is required to combat these crimes.
- 3) Throughout the survey, the majority of responding agencies had to estimate the number of investigations containing a cyber component as no actual statistics were readily available.
- 4) Penalties should be reviewed in addition to the laws surrounding the investigation and prosecution of computer-related crime due to its quickly-evolving nature.

In closing, the survey revealed a common sentiment by law enforcement. Based on comments from the survey, it appears investigators and prosecutors are routinely disconnected when dealing with crimes involving a cyber component. In the Greensboro area of judicial district 18, a unique partnership has been beneficial in dealing with the challenges posed by cases with a cyber component. An Assistant District Attorney works closely with the Greensboro Police Department on such cases. Because the ADA has undergone training at the national level, that person is more apt to handle prosecuting cases of this nature. The Analysis Center staff recommends that this collaboration model be examined more closely for potential replication throughout other areas of the state, ultimately providing both investigators and prosecutors with more confidence in the area of cyber crime.

Also, the Analysis Center staff recommends that consideration be given to establishing pilot sites for joint training sessions among neighboring judicial districts across the state. Joint training on these types of crimes would likely help alleviate some of the problems encountered by both investigators and prosecutors involved with such cases and would further support

collaborative partnerships between the two. Joint training could be used to address such topics as computer and technology terminology, methods of presenting computer-related cases, how to handle common issues brought forth by the defense, how to make current laws work in the prosecution of cases, and what investigators can provide the prosecution to strengthen a case. Agencies should work with the Governor's Crime Commission to attempt procurement of grant funds for confronting these crimes, whether used for training opportunities, equipment purchases or personnel positions.



APPENDIX

CYBER CRIMES SURVEY 2009

A SURVEY OF NORTH CAROLINAS' LAW ENFORCEMENT AGENCIES

1. How many total investigations did your agency conduct in 2008 (including both cyber and non-cyber)?
 - 1a. Please indicate if this is an Actual or Estimated Count.
2. How many of your agency's investigations contained a cyber component in 2008 (regardless of whether the cyber component was used in the prosecution)?
 - 2a. Please indicate if this is an Actual or Estimated Count.

If the response to question 2 is zero (0) skip to question 5.

3. Of those cases containing a cyber component, approximately what percentage (%) of those included the cyber component as part of the charges (e.g., someone accused of committing online credit card fraud is actually prosecuted under these charges rather than prosecuted as fraud only)?
 - 3a. Please indicate if this is an Actual or Estimated Count.
4. Approximately what percentage (%) of cases with a cyber component investigated by your agency in 2008 were comprised of the following: (total should equal 100%)
 - ____% Fraud (auction fraud, betting or investment fraud, credit/debit card),
 - ____% Forgery (currency, check, identification), or Larceny (theft of physical goods, intellectual property, telecommunications services)
 - ____% Violent crimes (assault, murder, rape, robbery)
 - ____% Criminal threatening (cyber bullying, stalking, harassment)
 - ____% Drug related (possession, trafficking)
 - ____% Online enticement of minors or Child pornography
 - ____% Cyber Attacks (intrusions, hacking, web defacements, unauthorized access) or Cyber squatting (registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else)
 - ____% Other (describe:) _____

5. How many investigators are in your office?
6. How many investigators, in your office, have received training to investigate crimes with a cyber component?
7. At what level has staff received training to investigate crimes with a cyber component? (Please check all that apply.)
- Local/intra district, or in-house training
 - State training (e.g., SBI/NC Justice Academy, Statewide Association)
 - Federal/National training (e.g., FBI, ICAC, ATF, ICE, or Nat'l Assns)
8. Please list any training not currently offered that would significantly increase your office's ability to investigate crimes with a cyber component.
9. Does your agency collect computer/electronic evidence during investigations?
- Yes
 - No
- 9a. If YES to question 9; for such seizures, does your agency have standard protocols established for the handling of computer/electronic data?
10. Does your agency have high speed internet access?
- Yes
 - No
11. On a scale of 1 (Does Not Impede) to 5 (Strongly Impedes), please indicate to what degree each of the following impedes the investigation of crimes with a cyber component:
- 11a. Lack of training for investigating crimes with a cyber component
- | | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
- 11b. Inability to trace and monitor Internet communications
- | | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
- 11c. Public apathy and lack of awareness towards crimes with a cyber component
- | | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
- 11d. Jurisdictional Issues
- | | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

11e. Lack of standard operating procedures for investigating crimes with a cyber component

1 2 3 4 5

11f. Lack of information sharing and intelligence

1 2 3 4 5

11g. Search warrant issues

1 2 3 4 5

11h. Lack of technical expertise due to staff turnover (promotions/reassignment, leaving for private sector)

1 2 3 4 5

11i. Other (please specify below)

1 2 3 4 5

12. Does your agency conduct any cyber crime prevention or awareness activities?

Yes

No

13. Is your agency involved in any official partnerships with other agencies or private entities to combat cyber crime?

Yes

No

14. What are your agency's priority outreach issues in relation to crimes with a cyber component?

15. Rate your opinion of the statement below:

Current General Statutes are adequate for prosecuting cyber crime.

Strongly Disagree Disagree Neutral Agree Strongly Agree

16. On a scale of 1 (Totally Unprepared) to 5 (Completely Prepared), overall how prepared is your agency to investigate cases with a cyber component in regards to the following areas?

16a. Training

1 2 3 4 5

16b. Personnel

1 2 3 4 5

16c. Equipment

1 2 3 4 5

16d. Law enforcement coordination with other agencies regarding investigative issues

1 2 3 4 5

The following questions pertain specifically to computer-mediated crime:

17. Has your agency ever investigated any cases in which a computer or electronic device mediated a traditional crime?

Yes

No

If "yes", describe or give examples.

18. Rate your opinion concerning each statement below:

18a. Current General Statutes are adequate for prosecuting crimes mediated by a computer.

Strongly Disagree Disagree Neutral Agree Strongly Agree

18b. Introduction of a bill to make it a crime to lure or entice another via electronic or any other means including the Internet for the purpose of committing a crime is needed in North Carolina (similar to New Jersey Legislative Bill A2864/S1429 passed during the 2004-2005 New Jersey State Legislative Session).

Strongly Disagree Disagree Neutral Agree Strongly Agree

18c. Penalties should be enhanced for traditional crimes mediated by a computer or electronic device (e.g., the use of Craigslist to facilitate a robbery should be considered an aggravating factor).

Strongly Disagree Disagree Neutral Agree Strongly Agree

18d. Our jurisdiction will experience an increase in computer-mediated crime in the next five years.

Strongly Disagree Disagree Neutral Agree Strongly Agree

18e. Law enforcement has little power to prevent or curtail computer-mediated crime.

Strongly Disagree Disagree Neutral Agree Strongly Agree

Please feel free to share any additional thoughts or comments regarding what steps policymakers or the Governor's Crime Commission (GCC) can take to lessen the extent of crimes with a cyber component.

GOVERNOR'S CRIME COMMISSION
1201 Front Street, Suite 200
Raleigh, North Carolina 27609
919.733.4564

www.ncgcd.org