Prosecuting Computer Crime in North Carolina: Assessing the Needs of the State's District Attorneys

Prosecuting Computer Crime in North Carolina: Assessing the Needs of the State's District Attorneys

North Carolina Governor's Crime Commission

North Carolina Criminal Justice Analysis Center

Douglas L. Yearwood and Richard Hayes

May,2003

Table of Contents

List of Tables and Figures

Executive Summary

The issue of cybercrime or computer related crimes slowly evolved during the last decade; however over the last three to four years this issue has received considerably more attention with members of the criminal justice system and the general public witnessing a real, or in many cases perceived, increase in the number of these types of crimes. Unfortunately, many law enforcement officials and judicial personnel originally found themselves behind the curve and have only recently begun to intensify and strengthen their investigative and prosecutorial efforts in this area.

This study sought to examine computer crime in North Carolina from the judicial perspective, specifically from the district attorney's point of view. The primary purpose of the study was to ascertain the specific needs of the district attorneys relative to computer related crimes. The research sought to answer program and policy relevant questions such as: How prepared are the state's prosecutors for handling these cases? What types of equipment, training and personnel needs do these offices have? What do the district attorneys see down the road regarding the future of these crimes in North Carolina? The study also sought to obtain a better indication of the nature and extent of cyber crime in North Carolina, i.e. capture case based statistics in this area.

A four part, 26 item questionnaire was designed in an effort to define and specifically pinpoint both the strengths and identifiable weaknesses of the D.A.s' offices in the area of computer, or cyber crimes. Surveys were mailed to each of the state's 39 district attorneys with follow-up phone calls being made after a low return rate was obtained from the original mail out. A total of 20 questionnaires were completed and returned by the state's prosecutors' offices producing a return rate of 51.3 percent.

Eight (40%) district attorneys noted that their offices did have individuals who currently possess specialized knowledge of computer crimes while the majority (60%) of the offices do not currently have any personnel with specialized knowledge in this emerging area.

Survey responses indicate that the majority of the computer crime cases, that have been prosecuted to date, are locally occurring events with both the plaintiff and defendant residing in the prosecutor's home jurisdiction. Fifty-eight percent of the survey participants noted that all of their computer related crime cases fell into this category; while the remaining 42 percent noted that their respective offices had prosecuted at least one computer crime case in which one of the parties was located outside of their judicial district. Those agencies that had prosecuted computer crime cases, that were outside of their judicial district,reported a total of 19 cases with an average of 2.7 cases per office.

As part of the needs assessment survey, each district attorney was asked to provide data on the number of computer related crimes which were filed within their judicial districts from fiscal year 1999/2000 to fiscal year 2001/2002. The most frequently reported type of computer crime was fraud (86.8%), followed by the use of a computer to lure children (4.7%) and identity theft (4.1%).

It should be noted that only seven (35%) prosecutors' offices were able to provide case filing statistics specific to computer crime cases. The majority of the respondents were unable to provide extracted statistics which disaggregated computer crimes from the total number of crimes for which their office had prosecuted cases during the three-year period.

The majority of the prosecutors reported that their offices' lacked adequate computer equipment and were lagging in technological capabilities. The average equipment rating for those prosecutors' offices that participated in the survey was 3.2 on a scale of 1 (totally unprepared) to 10 (completely prepared). Only two respondents noted that their respective offices were somewhat prepared as indicated by their assigned rankings of six or greater. No respondents felt that their offices' equipment and technological capabilities were completely adequate for prosecuting and managing computer crime cases.

Seventy percent of the survey participants specifically stated that their offices would need significant computer and network upgrades in order to be in a better position to successfully manage and prosecute cyber crime cases. Basic computer equipment, such as PCs, laptops and office suite software, were reported as the greatest need.

On average, the prosecutors reported a greater level of comfort in the personnel arena, compared to the equipment category. However, the overall average personnel rating was only 4.2 which is still lower than the scale midpoint of five. Twelve respondents (60%) reported rankings below the midpoint, five (25%) indicated a rating at the scale midpoint with the remaining three (15%) participants reporting a personnel preparedness score of six or greater.

Seven (53.8%) representatives from the participating prosecutors' offices described their greatest personnel need as more staff training. Four (30.8%) respondents noted a need for more personnel in addition to more training that is specific to the prosecution of computer related crimes. Both specialized personnel who can devote considerable time to investigating and prosecuting cyber crime cases, and specialized training, for at least the senior attorneys, are seriously needed and probably will be required if computer related crimes significantly increase in the future.

Only one respondent rated their office's training preparedness as being higher than five with 16 (80%) respondents reporting a score of less than five. On the average the survey participants reported a training score of 3.2 which is indicative of a low level of confidence in the degree of training that personnel have received, or in most cases have not received, in this area. Staff in the prosecutors' offices do not feel that they have been adequately trained for managing and prosecuting cybercrime cases.

Based upon this finding the respondents mentioned a strong need for more training in this area with recommendations being received for all levels of training from basic to advanced and as a part of attorneys' continuing legal education. Thirty-five percent of the participants noted a need for extensive training which would include not only senior attorneys but also involve other investigative and support staff. Twenty-five percent recommended expanding this training to involve local law enforcement personnel as well.

Comments on the extent of law enforcement and investigative support for prosecuting computer related crimes were more favorable with a higher average preparedness ranking of 4.2 being reported. Preparedness scores demonstrated a greater variance, when compared to the equipment, personnel and training scores with the score distribution ranging from two to 10. Despite the higher average score in this area it nonetheless remains below the scale midpoint with the prosecutors' offices possessing substantial needs in this area as well.

Sixty-seven percent of the survey participants noted an urgent need for law enforcement training with some suggesting a joint training initiative which would involve both members of the law enforcement community and staff of the prosecutors' offices. Respondents noted that while SBI agents are adequately trained, and normally called upon for assistance, there is a need to also train local law enforcement on handling and processing computer crime evidence and cases.

Seventy-five percent of those who responded to the survey thought that the current general statutes which address computer related crimes clearly delineated jurisdictional boundaries and issues, while the remaining 25 percent suggested that the statutes were not completely clear and did not adequately delineate all jurisdictional aspects of a computer related crimes case.

Members of the prosecutors' offices rated the adequacy of the current general statutes from a low of three to a high of 10 with a mean ranking of 5.4. Thus, as a general rule the respondents felt that the statutes were not necessarily inadequate, yet not completely adequate either.

As part of the survey the respondents were asked the following question: “In terms of the federal and state statutes, what is needed to enhance effective and efficient prosecution of computer crime cases?” Eight, or 40 percent, provided illuminating responses with concerns being expressed about the length of time required to prosecute these cases and also the lack of “real” penalties for violators. It was postulated that these lesser penalties and sanctions act as a deterrent to more aggressive and proactive law enforcement investigations and judicial prosecutions.

As a result of the study findings, four specific recommendations were offered in an attempt to alleviate the identified barriers to prosecuting computer related crimes. The need for both basic, and advanced training, equipment purchases and upgrades, as well as the suggestion to convene a legislative study committee on cyber crime were all recommended in an effort to improve the effectiveness and efficiency of the state’s prosecutors’ offices. Given a predicted increase in the nature, number and severity of these offenses, more specific and detailed case management information systems were also suggested in an effort to allow the prosecutors to monitor and exchange information on computer related crimes in the future.

Forward

Imagine, if you will, a venue where virtual communications and rapid transfers of information could be used in the commission of crimes. These crimes would range from petty annoyances to white collar crimes and even to murder. Is this media of criminality a condition of what Alvin Tofler refers to in his book The Third Wave *and society's dependence on technology or is it here today via the access granted computer users through the Internet? It is here, and are our laws concerning computer usage and the Internet in the commission of criminal acts, and the definitions of what constitutes a criminal act, lagging? Submitted below are a few examples of cyber crimes for your edification:*

Microchip Valley - Early this morning police arrested a 15 year old juvenile who was charged with deliberately and maliciously destroying the computer operating systems of the nation's largest financial institution. Authorities report that the child cracked the firm's encryption system, subverted several computer firewalls and other security programs and then unleashed a computer virus which eventually infiltrated sensitive financial records and ultimately deleted thousands of transaction records. The early morning raid on the juvenile's home surprised neighbors who stated that the child was a "bookworm" type but nonetheless enjoyed playing sports with the other children and teaching the younger kids in the neighborhood how to skateboard. In addition to computer paraphernalia authorities seized numerous technical computer manuals and notebooks replete with handwritten programming codes, many of which were obtained from the Internet. The child's parents thought that he did spend a lot of time on the computer but thought that he was only working on homework and surfing the "net". Bank officials could not be reached for comment.

Big City – Renewed feuding between two rival cross town gangs escalated to another level when two gang members were killed and several others, including an innocent bystander, were wounded during a late night drive-by shooting. Gang investigators believe the shooting occurred in retaliation as a result of last week's "cybercrime" turf battle in which members of the 43rd Street Crips hacked into the Hoover Park Bloods' website. Authorities have subpoenaed several Internet service providers to obtain access to e-mail communications in which the Hoover Park leader is alleged to have coordinated the drive-by shooting as well as openly bragged about several other gang related crimes. In a related story, the same service providers were hit with an injunction order to temporarily shut down their chat room service for failure to maintain adequate "cyber policing" and parental safeguards.

Reuters International Wire Service – Today at noon federal and local law enforcement executives will convene a press conference to announce the breakup of a major international child smuggling and Internet pornography ring which extended across the United States and involved numerous foreign citizens. Acting on a tip from a concerned chat room member, law enforcement officials raided the home of a 54-year old, married father of three, insurance company executive in suburban Michigan. The newly formed "multi jurisdictional cybercrime" task force seized numerous photographs and other evidence which leads a trail back to among others an oil executive in Bahrain, a doctor in Peru and the suspected ring leader, a top ranking military official in the Balkans. Future judicial proceedings are being described as murky and unresolved at this time given the international nature of the case and the uncertainty surrounding jurisdictional boundaries.

Anytown – In the latest twist in the on-going trial of a man suspected in the abduction and murder of a local 10 year old girl, defense attorneys argued that "cyber" chatting is protected speech,under the First Amendment, and that countless people assume fictional identities on the Internet. The defense's case was strengthened by satellite teleconference, press room testimony from a leading constitutional scholar who noted that the lack of clear legal definitions, jurisdictional issues and the absence of legal precedence in the area of " virtual society" cases are sufficient grounds for creating a reasonable doubt among the jury or sufficient grounds for an appeal. Prosecutors openly acknowledged that these issues, and the lack of legal training on electronic crimes and communications, could pose a significant barrier to their case but felt confident that the remaining physical evidence could sustain a conviction. Earlier in the week the judge failed to allow seized transcripts of the suspect's chat room activity with the victim as evidence citing improper search warrants and questionable evidence collection procedures. The ruling sparked intense debate in the General Assembly as victim advocates called for new legislation and documented protocols for law enforcement and court officials in order to bring the criminal justice system into the information age of the 21st Century.

Washington - The 2002 "Computer Crime and Security Survey" of about 500 public and private sector security officials, conducted by the Computer Security Institute (CSI) and the San Francisco FBI's Computer Intrusion Squad, found that 90 percent of respondents had detected an attack in the previous 12 months, with 80 percent reporting a resulting financial loss. The 44 percent of pollees willing or able to do so estimated total financial losses of nearly $456 million, or $2.04 million per respondent, up slightly from $2.02 million in 2001, and up significantly from $1.06 million in 2000. Seventy-four percent of those surveyed said their connection to the Internet was a "frequent point of attack," more than double the 33 percent who cited their internal systems as a frequent attack point. Just 37 percent of those attacked made a report to law enforcement officials, the survey found. Forty percent detected attacks originating externally, 40 percent detected denial of service hacks, and 85 percent were infected with a computer virus.

Cyber Crimes

> If cyberspace is a type of community, a giant neighborhood made up of networked computer users around the world, then it seems natural that many elements of a traditional society can be found taking shape as bits and bytes. With electronic commerce comes electronic merchants, plugged-in educators provide online education, and doctors meet with patients in offices on-line. It should come as no surprise that there are also cybercriminals committing cybercrimes. *(Jones Telecommunications and Multimedia Encyclopedia, 2002)*

Computers can be used as a weapon, a target or as accessories of crimes. Below is a listing of some of the more notable types of cyber crimes followed by short layman's definitions. The activities listed below are simply scratching the surface of the plethora of cyber crime activities currently taking place. However, a brief introduction of these activities must be discussed in developing an understanding of the scope of the problems related to cyber crime. Computers play an active role in the everyday lives of citizens, from retail check out scanners to internet purchases or communications, it is doubtless that each of us has been affected by some level of computer glitch not to mention some criminal activity. This broad discussion is designed to provide the reader with a general understanding of some of the more common activities as well as the not so common, but equally as detrimental to our society.

- Sales and investment fraud
- Information piracy, forgery, and counterfeiting
- Dissemination of offensive materials
- Electronic money laundering and tax evasion
- Electronic vandalism and terrorism
- Illegal interception and theft of telecommunications
- Electronic funds transfer fraud
- Child endangerment and sexual predatory behavior
- Computer crime boundaries (where jurisdiction begins and ends)

Sales and Investment Fraud:

One of the most obvious crimes committed via Internet connection is the sale of illegal, counterfeit, or non-existent goods or investment vehicles. Many online investment opportunities or equity trading companies have emerged over the past several years, making the need for a brick and mortar Investment Company less important to many people. Many legitimate retail and wholesale outlets have opted for a web presence. However, there are also unscrupulous individuals that will collect money and either not ship a product or ship something other than what the customer bargained for. Online auctions provide an opportunity for small and large-scale fraud. The buyer must beware whenever using the Internet to purchase any of these items. Original jurisdiction plays a large role in seeking justice when a fraud is committed via the Internet. Did the fraud take place in the location of the purchaser or the location of the seller? If the victim had to file a charge in another state, how likely would they be to pursue such an action. Computer sales fraud creates many legal questions that have yet to be adequately addressed by many jurisdictions.

Information Piracy, Forgery, and Counterfeiting:

Like in the previous category, several activities that are independent cyber crime activities have been coupled together. Information piracy refers to the illegal acquisition of information, be it commercial trade secrets or financial or medical information of individuals. Cyber forgery or counterfeiting refers to misrepresentations produced via computer, whether generated to a hard copy such as in making counterfeit money or submitted electronically using fraudulently obtained credit or credentials. An example would be someone building an electronic identification and history based on another person's credit and personal information. This is commonly referred to as *identity theft*.

Dissemination of Offensive Materials

Child pornography, long outlawed in paper form, has been distributed via the Internet. Pedophiles scan photos and keep volumes of pedophilia on their hard drives and compact discs. Of further concern are unwanted emails from pornographic and offensive web sites and the relatively easy access for children to view and acquire offensive materials be it pornography, hate literature or technological manuals for creating explosive devices.

Electronic Money Laundering and Tax Evasion

The disguise of illegally obtained funds in an effort to avoid detection and prosecution is defined as money laundering. However, using a computer via the Internet allows criminals to activate a series of transactions designed to hide assets whether from drug trafficking, organized crime, theft or other criminal activity. Keys to this type of activity are the layering and multiple movement of assets. It becomes hard to detect the legal from the illegal and the location of the illegal assets. The further (transactionally speaking) illegal assets are removed from the illegal source and overlapped with legitimate assets, describes electronic money laundering. It is also possible to use similar methodologies to hide assets from the Internal Revenue Service in efforts to avoid taxation. While electronic transfers do generate traceable documentation, when done at the speed of computer strokes rather that the delays involved in placing fund transfers in person or telephonically, the multiple movements and integration of other funds make tracing the movement of assets difficult.

Electronic Vandalism and Terrorism

Cyber attacks aimed at disabling or defacing Internet web pages or what is commonly referred to as "hacking" a web page is electronic vandalism. Electronic vandalism either impedes or prevents free access of business or the display of information. It could be defined as computer activity intended to interfere with and disrupt electronic commerce. Electronic terrorism *(cyber terrorism)*, extrapolated from the Federal Bureau of Investigation's definition of terrorism, "is the improper use of electronic property (information in a database) utilized to intimidate or coerce the government, business or individuals to achieve political or social goals". A good example would be if a hacker obtained entrance into the Federal Aviation Administration's computer system and brought down the air traffic control computers. Flights in the air would be unsafe and scheduled flights for passengers, goods, and emergency provisions would be brought to a halt.

Illegal Interception and Theft of Telecommunications

The use of computers to intercept and/or fraudulently obtain telecommunication services has been on the rise. Computer Security Institute surveys indicate that most telecommunications businesses are working diligently to prevent these thefts. As with most computer related crime, all users are victimized via higher rates charged by the company to cover losses to computer theft. The interception of telecommunications also invades personal, business and governmental privacy. Sometimes called "phreaking", hackers also attempt to illegally obtain information from telephone companies that would enable them to receive free telephone system access for their computers and for personal voice communications.

Electronic Funds Transfer Fraud

Electronic fund transfers generally refer to the process organizations use to transmit payment instructions to a financial institution for payment of employees, third parties or other entities. Fund transfer fraud relates to the fraudulent access of funds, either existent or non-existent, from an institution delegated to enact such a transfer, or to obtain through false information an electronic transfer of funds for an illegal benefit.

Child Endangerment and Sexual Predatory Behavior

One of the growing concerns of families is the danger of the Internet and uncontrolled chat rooms which children may freely join. Original concerns were with the availability to children of materials found on the Internet that are either pornographic, obscene, distasteful or arousing the prurient interest of young minds. However, chat rooms have opened our society's eyes to a more violent and vicious scourge on our youth, adults who prey on children via chat room communications. Chat rooms are synonymous with the now no longer common party line on a telephone exchange in the first half of the 20th century. Many people can actively join in communications with people in the cyber room. If someone finds the messages of another person interesting, or they are acquaintances, they can P.M. To be *P.Med* means to be sent a personal message. Theses are designed to remove the individuals from the open chat room to a personal conversation. Pedophiles can start conversations with children and lure them into dangerous conversations and even into personal meetings. Parents have always warned their children of the dangers of talking to strangers, but today the strangers are talking to our children in our own homes via personal computers. While the conversations may not be illegal they can lead to actual meetings which place the children in greater danger of being assaulted, abducted and even murdered.

Introduction/Study Rationale

The issue of cybercrime or computer related crimes slowly evolved during the last decade; however, over the last three to four years this issue has received considerably more attention with members of the criminal justice system and the general public witnessing a real, or in many cases perceived, increase in the number of these types of crimes. High profile media cases, Internet scams and hoaxes as well as an increase in the number of academicians who have directed their research in this area have all coalesced and brought this issue to the attention of both politicians and policy makers.

Unfortunately, many law enforcement officials and judicial personnel originally found themselves behind the curve and have only recently begun to intensify and strengthen their investigative and prosecutorial efforts in this area. Training conferences have been held and investigative manuals and technological tools have been designed and created in response to this growing concern. Some larger urban jurisdictions have formed highly specialized cyber crime units with other smaller suburban and rural jurisdictions giving these investigative and prosecutorial units more serious consideration than they did as recently as three to four years ago.

This study sought to examine computer crime in North Carolina from the judicial perspective, specifically from the district attorney's point of view. The primary purpose of the study was to ascertain the specific needs of the district attorneys relative to computer related crimes. The research sought to answer program and policy relevant questions such as: How prepared are the state's prosecutors for handling these cases? What types of equipment, training and personnel needs do these offices have? What do the district attorneys see down the road regarding the future of these crimes in North Carolina? The study also sought to obtain a better indication of the nature and extent of cyber crime in North Carolina, i.e. capture case based statistics in this area.

It is anticipated that this exploratory study will be a first step for addressing the issue of computer related crime in North Carolina. If findings indicate that computer crime is not pervasive, or currently viewed as problematic, what can the state's policy makers do to insure that it remains so in the future? If findings indicate that computer crime is a problem or concern, and that the district attorneys have specific needs in this area, then hopefully the study will generate further discussions; discussions which have the potential to shape policy, program development and legislation.

Methods

Survey Instrument

A four part, 26 item, questionnaire was designed in an effort to define and specifically pinpoint both the strengths and identifiable weaknesses of the D.A.s' offices in the area of computer, or cyber crimes. Part one of this needs assessment included questions which sought to ascertain the extent to which the state's prosecutors' offices possessed individuals who had either specific training or knowledge of computer related crimes. Questions also dealt with the clarity of the current statutes as they relate to prosecuting and managing computer crimes, and asked respondents to identify how many cyber crimes their respective offices have prosecuted, and the number internal and external to their prosecutorial districts.

Part two contained a table or chart which listed numerous types of computer related crimes with the respondents being asked to identify the number of cases prosecuted within the last three fiscal years, and the disposition of those cases. Part three contained questions which were designed to elicit the extent to which the prosecutors' offices were prepared to adequately prosecute computer related crimes. Respondents were asked to rate their respective offices in the areas of equipment, training, personnel and law enforcement coordination. Open-ended questions were included to allow the participants to document their specific needs in each of these areas.

The final section of the survey addressed the future of computer related crimes and included items on barriers to successful prosecution, the perceived future impact of cybercrime, the use of investigative grand juries with these types of cases, and allowed the respondents to list any other needs or issues which were deemed to be relevant.

Study Sample

Surveys were mailed to each of the state's 39 district attorneys with follow-up phone calls being made after a low return rate was obtained from the original mail out. These follow-up phone calls bolstered the overall return rate by approximately 50 percent and produced a more even distribution of responses reflecting both prosecutors' offices in rural and urban areas, as well as creating a greater degree of geographical representation from offices throughout the state.

Results

A total of 20 questionnaires were completed and returned by the state's prosecutors' offices. This equated to a 51.3 percent response rate with responses being obtained from prosecutors whose offices covered both urban and rural jurisdictions, as well as offices located within all three major geographical areas of North Carolina.

Part one of the survey contained a series of questions in which the survey respondents were asked to delineate a profile of their respective offices and specify the extent to which staff were knowledgeable in the area of cyber crime. The respondents were also asked to provide basic data regarding the number of computer crime cases which their respective offices have prosecuted and to document the number of cases involving parties outside of their prosecutorial districts.

Eight (40%) district attorneys noted that their offices did have individuals who currently possess specialized knowledge of computer crimes while the majority (60%) of the offices do not currently have any personnel with specialized knowledge in this emerging area.

Of those eight prosecutors' offices, that reported staff with specialized computer crime knowledge, 75 percent noted that those individuals had received specific instruction on the unique search and seizure aspects of computer crime. Only two prosecutor's offices had staff who they identified as being specialists in this area. One office reported the presence of one specialist while the other office declared that they had three attorneys who were considered to be specialists, or subject matter experts, in the area of computer related crime. Only one respondent noted that their prosecutor's office had plans to develop a specialized cybercrime unit within the near future.

Survey responses indicate that the majority of the computer crime cases, that have been prosecuted to date are locally occurring events with both the plaintiff and defendant residing in the prosecutor's home jurisdiction. Fifty-eight percent of the survey participants noted that all of their computer related crime cases fell into this category while the remaining 42 percent noted that their respective offices had prosecuted at least one computer crime case in which one of the parties was located outside of their judicial district. Those agencies that had prosecuted computer crime cases outside of their judicial district reported a total of 19 cases with an average of 2.7 cases per office.

Thirty-seven percent of the responding prosecutors reported that their offices had prosecuted computer related crimes which involved at least one out-of-state party, either plaintiff or defendant. Four cases of this type were reported with an average of 1.3

cases per responding prosecutor's office. Out of state cases involved parties from Texas, Virginia and Kentucky.

None of the participating district attorneys' offices had prosecuted any cases which transcended national boundaries; i.e. no international cases were reported.

As part of the needs assessment survey each district attorney was asked to provide data on the number of computer related crimes which were filed within their judicial districts from fiscal year 1999/2000 to fiscal year 2001/2002. As Table 1 demonstrates, the most frequently reported type of computer crime was fraud (86.8%), followed by the use of a computer to lure children (4.7%) and identity theft (4.1%).

Table 1 Computer Related Criminal Case Filings FY 1999/2000 - 2001/2002

Criminal Offense	Number Filed	Percent
Fraud	1,392	86.8 %
Use of computer to lure children	75	4.7 %
Identity Theft	66	4.1 %
Data Theft	43	2.7 %
Unauthorized computer access	12	.7 %
Cyber stalking	10	.6 %
Pornography	6	.4 %
Computer sabotage	0	0 %
External or unauthorized system shutdowns	0	0 %
Total	1,604	100 %

It should be noted that only seven (35%) prosecutors' offices were able to provide case filing statistics specific to computer crime cases. The majority of the respondents were unable to provide extracted statistics which disaggregated computer crimes from the total number of crimes for which their office had prosecuted cases during the three-year period. Several respondents provided comments regarding this portion of the questionnaire including:

☛ " No such statistics have been maintained by this office"

☛ " We have no way of pulling these statistics "

☛ " I do not know the numbers. The majority of what we see in our county is fraud, identity theft and pornography. We have had a handful of use of a computer to lure children and a few cyber stalking cases."

Thus the data presented in Table 1 provide a ***minimum*** number of computer crime cases in North Carolina with some of the information representing an estimate or best "guess-estimate" on the part of the prosecutors' offices. Thus generalizations based upon this information should be approached with caution. It is difficult to ascertain the extent to which this low, or minimum, number of case filings reflects the actual number of true computer crime cases or a lack of aggressive investigation and prosecution or a statistical reporting issue in which raw administrative data on these types of cases is not readily available.

The third section of the survey addressed the specific strengths and weaknesses of the prosecutors' offices on a range of computer crime, or cyber crime, issues. Respondents were encouraged to rank their respective offices on a 10 point scale ranging from one (totally unprepared or inadequate) to 10 (totally prepared or adequate). Each prosecutor was given the opportunity to rate their agency's level of preparedness and to discuss their specific needs relative to computer crime for the following areas: equipment, personnel, training, law enforcement coordination, and the adequacy and utility of the general statutes for prosecuting cyber crime cases.

Figure 1 Level of Preparedness - Equipment

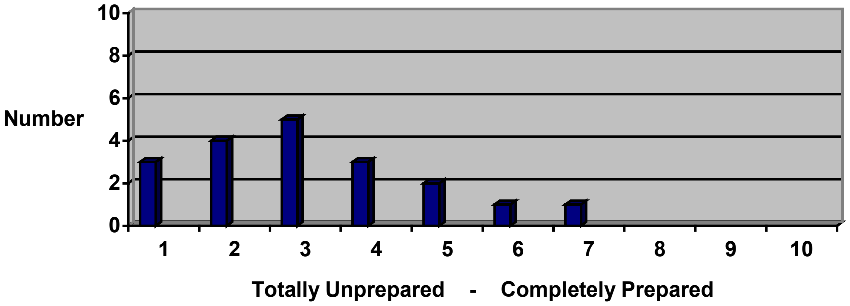
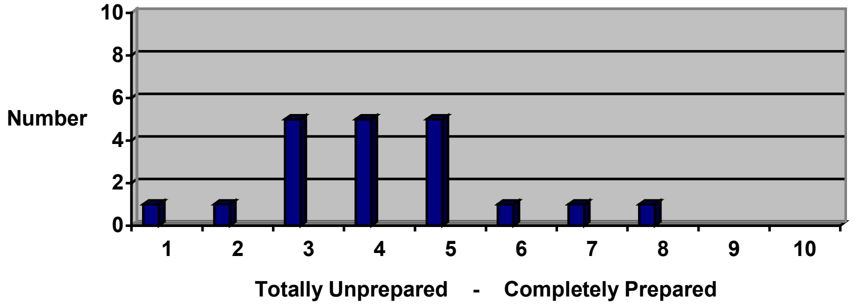


Figure 1 presents the response distribution for the level of equipment preparedness as reported by the survey participants. As the figure reveals, the majority of the prosecutors reported that their offices lacked adequate computer equipment and were lagging in technological capabilities. The average equipment rating for those prosecutors' offices that participated in the survey was 3.2. Only two respondents noted that their respective offices were somewhat prepared as indicated by their assigned rankings of six or greater. No respondents felt that their offices' equipment and technological capabilities were completely adequate for prosecuting and managing computer crime cases.

Seventy percent of the survey participants specifically stated that their offices would need significant computer and network upgrades in order to be in a better position to successfully manage and prosecute cyber crime cases. Basic computer equipment such as PCs, laptops and office suite software were reported as the greatest need. A few respondents mentioned the need for advanced evidence management and presentation equipment, such as ELMO which allows for the visual electronic presentation of multiple exhibits. But for the most part basic equipment upgrades are needed before introducing complex equipment and advanced computer crime technologies into the prosecutors' offices and courtrooms.

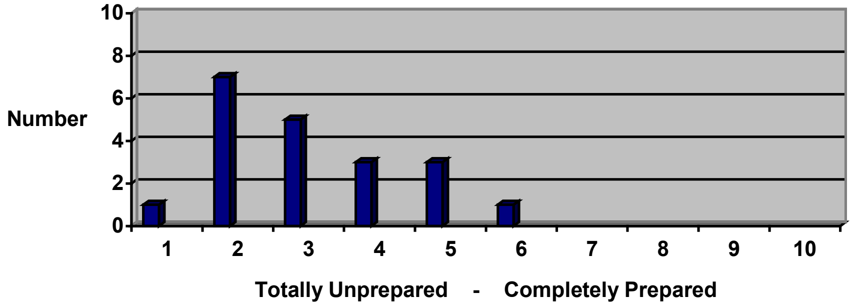
Figure 2 presents the extent to which the district attorneys' offices felt that their staff was adequately prepared for managing and prosecuting computer crime cases. On average the prosecutors reported a greater level of comfort in this area compared to the equipment category however, the overall average personnel rating was only 4.2 which is still lower than the scale midpoint of five. Twelve respondents (60%) reported rankings below the midpoint, five (25%) indicated a rating at the scale midpoint with the remaining three (15%) participants reporting a personnel preparedness score of six or greater.

Figure 2 Level of Preparedness – Personnel



Seven (53.8%) representatives from the participating prosecutors' offices described their greatest personnel need as more staff training. Four (30.8%) respondents noted a need for more personnel in addition to more training specific to the prosecution of computer related crimes. Both specialized personnel who can devote considerable time to investigating and prosecuting cyber crime cases, and specialized training for at least the senior attorneys are seriously needed and probably will be required if computer related crimes significantly increase in the future.

Figure 3 Level of Preparedness – Training



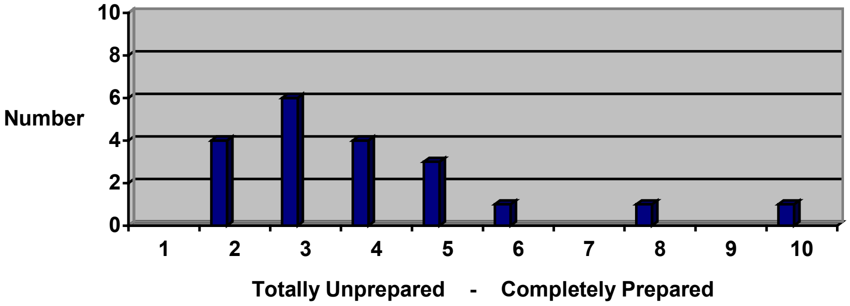
As Figure 3 depicts, only one respondent rated their office's training preparedness as being higher than five with 16 (80%) respondents reporting a score of less than five. On the average the survey participants reported a training score of 3.2 which is indicative of a low level of confidence in the degree of training that personnel have received, or in most cases have not received, in this area. Staff in the prosecutors' offices do not feel that they have been adequately trained for managing and prosecuting cybercrime cases.

Based upon this finding the respondents mentioned a strong need for more training in this area with recommendations being received for all levels of training from basic to advanced and as a part of attorneys' continuing legal education. Thirty-five percent of the participants noted a need for extensive training which would include not only senior attorneys but also involve other investigative and support staff. Twenty-five percent recommended expanding this training to involve local law enforcement personnel as well. Specific recommendations suggested both substantive and procedural training and noted the need to understand basic information on how computer crimes are perpetrated, the dynamics of the Internet, file transfer methods and telecommunication protocols. It was suggested that procedural training should, at a minimum, include information on search and seizure, evidence management and presentation, and also technology training for electronically presenting evidence to the jury.

Comments on the extent of law enforcement and investigative support for prosecuting computer related crimes were more favorable with a higher average preparedness ranking of 4.2 being reported. Preparedness scores demonstrated a greater variance, when compared to the equipment, personnel and training scores with the score distribution ranging from two to 10 (Refer to Figure 4). Despite the higher average score in this area it nonetheless remains below the scale midpoint with the prosecutors' offices possessing substantial needs in this area as well.

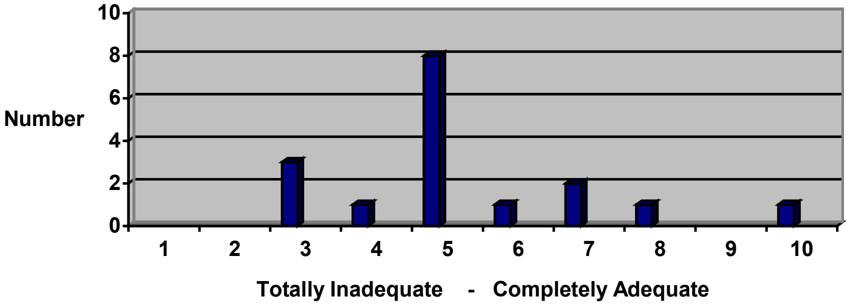
Sixty-seven percent of the survey participants noted an urgent need for law enforcement training with some suggesting a joint training initiative which would involve both members of the law enforcement community and staff of the prosecutors' offices. Respondents noted that while SBI agents are adequately trained, and normally called upon for assistance, there is a need to also train local law enforcement on handling and processing computer crime evidence and cases. The need for training local law enforcement officers was corroborated by one respondent who noted that their office's support was excellent because each of the local law enforcement agencies in their jurisdiction had personnel who were well versed on computer crime issues.

Figure 4 Level of Preparedness – Law Enforcement & Investigative Support



Seventy-five percent of those who responded to the survey thought that the current general statutes that address computer related crimes clearly delineated jurisdictional boundaries and issues, while the remaining 25 percent suggested that the statutes were not completely clear and did not adequately delineate all jurisdictional aspects of a computer related crimes case.

Figure 5 Level of Adequacy – General Statutes



Members of the prosecutors' offices rated the adequacy of the current general statutes from a low of three to a high of 10 with a mean ranking of 5.4. Thus, as a general rule the respondents felt that the statutes were not necessarily inadequate, yet not completely adequate either (Refer to Figure 5).

As part of the survey the respondents were asked the following question: " In terms of the federal and state statutes what is needed to enhance effective and efficient prosecution of computer crime cases?" Eight, or 40 percent, provided illuminating responses with concerns being expressed about the length of time required to prosecute these cases and also the lack of "real" penalties for violators. It was postulated that these lesser penalties and sanctions act as a deterrent to more aggressive and proactive law enforcement investigations and judicial prosecutions. Other comments centered on expanding current state law to allow for a "good faith" exception in searches and seizures, clarifying and strengthening existing child pornography laws, and the need to clarify jurisdictional issues and promote more collaborative investigative and prosecutorial endeavors.

Based on the comments of the prosecutors and their staff the most significant obstacle, or barrier, which limits their abilities is the lack of training on this emerging crime issue. An overwhelming number of comments were received about the lack of training in this area and on how this handicaps the prosecutors from performing their roles in the most effective and efficient manner. Other barriers and obstacles which were delineated are highlighted below:

- " Takes a lot of time to prosecute one of these cases "
- " Not enough law enforcement officials assigned to cases "
- " Understaffed prosecutors "
- " Witnesses may be out of state – too expensive to prosecute "
- " Difficult to prove who was actually in front of the computer sending/receiving information "
- " High caseload already and lack of familiarity with statutes makes it difficult to prosecute "
- " Lack of law enforcement interest "
- " Lack of AV equipment and equipment in general "

Respondents were also given the opportunity to offer recommendations on how to alleviate, or at least minimize, these barriers to investigating and prosecuting computer crime cases. Few specific and detailed recommendations were offered with more global comments being received. These clustered around offering more training, updating existing equipment, purchasing new state of the art equipment, needed technological peripherals, improving federal and state cooperation, and adding more staff who would specialize in computer crime case investigations and prosecutions. Offering training through the Conference of District Attorneys and establishing an interstate network to assist in the prosecution of cases were two of the more specific recommendations which were suggested. It was also suggested that the establishment of specialized prosecutors, who would work statewide until local capabilities are developed and strengthened, should be given consideration.

Recommendations specific to the Governor's Crime Commission (GCC) included conducting a joint training session with the Conference of District Attorneys. It is also suggested that federal grant funds be used to purchase specialized equipment and for financing training. Funds could also be offered as financial assistance for the specialized statewide prosecutor plan should it be implemented.

Eighty-one percent of those who responded to the survey strongly asserted that computer related crimes, or cyber crimes, would exert a strong, sizeable and significant impact on North Carolina's prosecutors five years from now. Specific comments are elucidated below:

- " Increasing even in rural districts "
- " Will increase a lot with widespread use of the Internet and society becoming more computer dependent "
- " Seen an increase in number of investigations, expect to prosecute some in the near future "
- " Will see increase in Identity Theft "
- " Will grow, i.e. specifically financial and sexual exploitation cases "
- " A very significant increase "
- " Moderate increase, more in larger areas "
- " Not much, Feds should handle most of it "

Discussion/ Policy Implications and Recommendations

Study findings, comments from the prosecutors' staff and the low preparedness scale scores all suggest that the state's district attorneys' offices are currently not capable of managing and prosecuting computer crime cases at the same level of effectiveness and efficiency as they have demonstrated with non-computer related criminal cases. Only 35 percent of the offices were able to provide case statistics specific to computer related crimes. Sixty percent of the surveyed offices reported that their current personnel do not have adequate and specialized knowledge for managing and prosecuting cyber crime cases. Average preparedness scores were low for all study factors with the lowest scores being reported in the areas of equipment and training.

Given the fact that 81 percent of the respondents predicted a sizeable increase in both the number of anticipated cases, and their projected impact on the prosecutors' offices, the following recommendations are offered. These suggestions are presented in an effort to proactively address the issue of computer crime before it becomes an even more urgent issue or at the extreme a significant crisis and burden on the prosecutors.

Recommendation # 1

In-state computer crime training should become a priority with basic to advanced levels of instruction being available. Courses specific to the needs of the state's prosecutors should be developed with an emphasis on the unique aspects of managing and prosecuting these types of cases. This training should be offered to, at a minimum, the state's district attorneys and their senior staff, and if feasible be expanded to include all assistant district attorneys and others who will be involved with any computer related criminal cases. Joint training with local and state law enforcement officials is also strongly encouraged and could be offered through a conference format. The Administrative Office of the Courts, the Conference of District Attorneys, the Institute of Government, and the North Carolina Criminal Justice Academy are possible agencies which could play a role in developing and administering this training. Training should be offered on a continual basis to reflect emerging trends, new technologies and legal updates.

Attendance at national training courses and seminars should be encouraged especially for members of those prosecutors' offices which are experiencing an increase in the number of computer crime cases. The National District Attorneys Association offers computer crime training courses such as Cybersleuth I and a more advanced Cybersleuth II. Other national training courses are offered by the FBI, the International Association of Computer Investigative Specialists (IACIS), and the Federal Law Enforcement Training Center's Financial Fraud Institute (FLETC/FFI).

Recommendation # 2

The needs assessment survey clearly demonstrated the inadequacies of many of the state's prosecutors' offices in terms of their existing computer equipment and the lack of current technological necessities which are needed to successfully prosecute cyber crime cases. Securing funding will remain a challenge as the current recession will make this an even more difficult proposition. Efforts should be directed at making equipment procurement and computer upgrades a top priority for the state's prosecutors with the need for such equipment transcending the issue of computer related crime and being required for the normal day to day operations of these offices.

The state's prosecutors are encouraged to work closely with the Governor's Crime Commission to obtain the latest information on available funding sources and to receive technical assistance should they decide to submit a grant pre-application for addressing the equipment needs associated with computer crime.

Recommendation # 3

Consideration should be given to empanelling a legislative study commission which would investigate the issue of computer crime as it intersects e-commerce and e-government operations. The current general statutes regarding computer crime should be reviewed as well as the range of available sanctions, fines and other penalties which are proscribed for these offenses.

Recommendation # 4

The lack of available case statistics on computer related crimes could pose future problems when financial, personnel and time management decisions are based upon case management, administrative and statistical data. Improving, or expanding, existing case management information systems to enable the prosecutors to extract relevant computer crime data could be beneficial and allow them to ascertain how computer crime cases impact their existing workloads and court dockets.

Glossary

back door -- a vulnerability intentionally left in the security of a computer system or its software by its designers
Biometrics -- the use of a computer user's unique physical characteristics -- such as fingerprints, voice, and retina -- to identify that user
black hat -- a term used to describe a hacker who has the intention of causing damage or stealing information
bypass -- a flaw in a security device
ciphertext -- data that has been encrypted
Computer Emergency Response Team (CERT) -- an organization that collects and distributes information about security breaches
countermeasure -- any action or device that reduces a computer system's vulnerability
cracker -- a term sometimes used to refer to a hacker who breaks into a system with the intent of causing damage or stealing data
cracking -- the process of trying to overcome a security measure
cryptography -- protecting information or hiding its meaning by converting it into a secret code before sending it out over a public network
crypto keys -- the algorithms used to encrypt and decrypt messages
Cybercrime -- crime related to technology, computers, and the Internet
cyber stalking --
decrypt -- the process of converting encrypted information back into normal, understandable text
denial of service (DoS) -- an attack that causes the targeted system to be unable to fulfill its intended function
digital signature -- an electronic equivalent of a signature
domain name -- the textual name assigned to a host on the Internet
dumpster diving -- looking through trash for access codes or other sensitive information
email -- an application that allows the sending of messages between computer users via a network
encryption -- the process of protecting information or hiding its meaning by converting it into a code
firewall -- a device designed to enforce the boundary between two or more networks, limiting access
hacker -- a term sometimes used to describe a person who pursues knowledge of computer and security systems for its own sake; sometimes used to describe a person who breaks into computer systems for the purpose of stealing or destroying data
hacking -- original term referred to learning programming languages and computer systems; now associated with the process of bypassing the security systems on a computer system or network
high risk application -- a computer application that, when opened, can cause the user to become vulnerable to a security breach
hijacking -- the process of taking over a live connection between two users so that the attacker can masquerade as one of the users
host -- a computer system that resides on a network and can independently communicate with other systems on the network

Hypertext Markup Language (HTML) -- the language in which most webpages are written
information security -- a system of procedures and policies designed to protect and control information
Internet -- a computer network that uses the Internet protocol family
Internet Relay Chat (IRC) -- a large, multiple-user, live chat facility
Internet service provider (ISP) -- any company that provides users with access to the Internet
intranet -- a private network used within a company or organization that is not connected to the Internet
intrusion detection -- techniques designed to detect breaches into a computer system or network
IP spoofing -- an attack where the attacker disguises himself or herself as another user by means of a false IP network address
keystroke monitoring -- the process of recording every character typed by a computer user on a keyboard
leapfrog attack -- using a password or user ID obtained in one attack to commit another attack
letterbomb -- an email containing live data intended to cause damage to the recipient's computer
malicious code -- any code that is intentionally included in software or hardware for an unauthorized purpose
one-time password -- a password that can be used only once, usually randomly generated by special software
packet -- a discrete block of data sent over a network
packet sniffer -- a device or program that monitors the data traveling over a network by inspecting discrete packets
password -- a data string used to verify the identity of a user
password sniffing – an examination of data traffic in an attempt to find passwords for use in entering a system
pen register -- a device that records the telephone numbers of calls received by a particular telephone
phracker – someone who combines phreaking and hacking
phreaker -- a person who hacks telephone systems, generally to obtain codes for making free telephone calls
piggyback -- gaining unauthorized access to a computer system via another user's legitimate connection
piracy -- the illegal copying of copyrighted software, music, or movies.
Pretty Good Privacy (PGP) -- a freeware program designed to encrypt email
probe -- an effort to gather information about a computer or its users for the purpose of gaining unauthorized access later
risk assessment -- the process of studying the vulnerabilities, threats to, and likelihood of attacks on a computer system or network
smart card -- an access card that contains encoded information used to identify the user
sniffer -- a program designed to capture information across a computer network
social engineering -- term often used to describe the techniques virus writers and hackers utilize to trick computer users into revealing information or activating viruses
spam -- unsolicited commercial email
spoofing -- the process of disguising one computer or user to look like another

trap and trace device -- a device used to record the telephone numbers dialed by a specific telephone
Trojan horse -- an apparently innocuous program that contains code designed to surreptitiously access information or computer systems without the user's knowledge
virus -- a computer program designed to make copies of itself and spread itself from one machine to another without the help of the user
war dialer -- software designed to detect dial-in access to computer systems
warez – a slang term used for illegal or pirated software
white hat hacker -- a hacker who has neither criminal or malicious intentions; generally a computer security expert hired by a corporation to test their system
wiretapping -- the interception of electronic communications in order to access information
worm -- a computer program that copies itself across a network
zombie machine – for computers always online, such as with Road Runner, hackers are able to use these machines, in the absence of firewalls or other protective devices, to impersonate or leave a trail pointing to the zombie machine. This sort of misdirection of origination provides a shield for experienced hackers.