Partnering With Others To Address Cybercrime

Gerald Konkler

As should be evident from the other chapters in this volume, cybercrime is a present and increasing concern for policing and society. With existing levels of personnel, expertise, and equipment, most agencies are hard-pressed to address even the current incidence level of these crimes. Most police agencies do not have the resources to effectively or efficiently detect, prevent, or investigate many technology-related crimes, particularly cybercrime. This paper will suggest some strategies for local police to more effectively address cybercrime in the future by identifying and utilizing resources both without and outside their agency.

Some assumptions:

- → The use of computers in criminal activity will continue to increase.
- → Local agencies are behind the curve in addressing cybercrime and computer related crime.
- → Local agencies will continue to investigate cybercrimes at least to the degree they are capable (i.e., we will not totally abdicate our responsibilities to citizens and will attempt to respond in some manner to these types of calls for service).

The policing industry has historically resisted involving outside entities in policing efforts. Coupled with the sluggish nature exhibited by the police in adapting to change and embracing technology (or at least, resistance to technology that does not directly relate to catching criminal offenders), and there is little wonder there is much room for improvement in how policing responds to cybercrime and computer related crime. It has been said that every crisis brings opportunity. Policing has an opportunity to partner with others and improve services to the community.

For decades, community policing has pushed us toward involving others in policing efforts. In some cases, to varying degrees, we have at least given lip service to the value of the expertise and opinions of others. In order to effectively and efficiently address computer-related crime, policing must become more willing to involve others by utilizing their expertise while still protecting the rights of those accused and adhering to the vision, mission, and values of the agency.

An initial question might be whether an agency needs a specialized unit or section devoted to investigating cybercrimes. While this is a decision driven by agency size, local politics, and resources, it seems axiomatic that citizens who need to report a crime will at least start with their local police agency. If an agency opts not to create a special unit/section/position, at the very least it will need to identify resources or agencies to whom the agency can refer those who report cybercrime.

At a conference held by the FBI in July 2000, it was forecast that more police departments, even smaller agencies, would have personnel trained in the investigation of computer crimes

(Futuristics, 2000)[24]. While this has likely occurred, one could question whether the levels of training are sufficient. Are agencies simply using decoys to troll for online predators? As laudable and necessary as this may be, it does not require the level of training that is necessary to address cyber scams committed by organized crime syndicates or sophisticated denial of service attacks or to do forensic examinations of computers to search for evidence.

This then leads to another question to be answered by the agency: what level of expertise should be (or can be) identified or developed internally? Does the agency have the ability to investigate "cybercrime," i.e., where a computer is used to attack another computer or network? The investigation of denial of service attacks would be an example and, as noted, would require a high level of expertise. Or should the agency concentrate on "computer related crime," those instances where the computer is used to store evidence of a crime or used as a communication tool to commit a more traditional crime? Examples of this type include fraud schemes, child pornography, and online sexual predators. Does the agency have the expertise to conduct forensic examinations of computer systems? Obviously the effective and efficient investigation of either of the types of crimes will hinge on the ability to do so. These are questions that the agency head should consider before the need arises.

Whether an agency has a unit or elects to create a section, it is imperative that they be aware of what expertise currently exists in the agency. Without a doubt, police have more technologically savvy personnel now than in the past (as does society—and as does the criminal element!). Smaller agencies perhaps will already be aware if they have someone already employed who has computer expertise and/or a technical background. Larger agencies may have personnel who possess needed skills or at least a level of skill which the agency can enhance to meet their needs. Some agencies may have self-taught personnel who have some expertise in computers. Unless the agency has a personnel management system that identifies those with various skills/talents, an agency-wide survey of talents should be considered. Because of their interest in the subject matter, these personnel may have contacts with others in the field, either practical or academic. These contacts can be beneficial in establishing partnerships.

Even if skilled personnel are available internally, levels of expertise vary and may not be sufficient for the more complex investigations. To effectively deal with the variety of cybercrimes, an agency needs to have access to forensic computing experts and equipment and experts in tracking other types of cybercrime. Hence, there is still a need for partnerships. There

[24] In addition to identifying the trend, the Conference also suggested strategies. Two strategies are noteworthy and pertinent to the topic. First, the Conference stated one of the highest strategies for the future of policing was for agencies to develop tools and expertise in the investigation of cybercrimes. Second, it was suggested that agencies form partnerships with academic institutions (in a variety of disciplines) to educate and train personnel in emerging technologies which impact the policing profession.

have been well-publicized incidents where agencies with limited expertise and/or equipment have attempted to examine computers and allegedly overlooked critical evidence (Ellis, 2004).[25]

Whatever the level of involvement in cyber investigations, an agency is obligated to collect evidence in a lawful and competent manner. Evidence of traditional crimes as well as cybercrimes is frequently found on computers. Officers who are involved in virtually any investigation could face the risk of destroying evidence by either illegally seizing it or causing it to be physically destroyed because of traps laid by the suspect. Agencies that are accredited through CALEA are required to have a written directive that establishes procedures for the seizure of computer equipment and other electronic data storage devices. Improper recovery can result in the loss of data (Standards, 83.2.5, 2006). If an agency does not possess a level of expertise, local resources, private or public, must be identified.

STINGS

Apprehending online predators is an area where policing has received assistance from other entities. Perverted Justice is a private group that was started with a goal of cleaning up internet chat rooms. It has evolved to what they call a lead internet resource for combating sexual predators online. This group uses volunteers posing as children to go into chat rooms and wait for sexual predators to initiate conversations with them. As viewers of NBC's Dateline are aware, these contacts can evolve into actual attempts by the predators to meet their target and arrests of these predators (Perverted Justice, 2006). Initially, the television show did not involve law enforcement and simply broadcast Chris Hansen's interview with the offender in a sort of 'public shaming' reminiscent of medieval stocks. Because of viewer complaints/comments about letting the potential pedophiles escape punishment, police were involved and began arresting suspects as they left the house used in the sting. (McCollum, 2007). This resulted in an alliance between NBC, Perverted Justice, and various local police agencies that opted to assist in these televised stings.

It could be argued that there has

[25] For example, see "Mom's sleuthing helped find missing daughter," by Ellis above. In that case a 14 year old female was reported missing. The Sheriff's Office was criticized for treating the case as a runaway rather than an Internet related abduction and for failing to conduct a forensic examination of the girl's computer even though it was believed she was with someone she'd met online. The mother checked websites the girl had visited and ultimately contacted Perverted Justice. The director of Perverted Justice expressed shock that a forensic examination of the girl's computer had not been conducted. Perverted Justice contacted the Internet provider who would only provide information to the law enforcement agency. At the urging of Perverted Justice, the investigator contacted the Internet provider and discovered the name of the suspect. It was discovered that the girl had been kidnapped by someone she had met when she posted her poetry online. The suspect was charged with kidnapping, rape of a child, and sexual exploitation of a minor. The investigator noted that they had difficulty examining the girl's computer because the County's firewalls blocked many of the sites the girl visited.

been a blurring of the line between television news and 'show business.' Now, the lines between show business, law enforcement, and policing have become muddied. To long time observers of the police industry, it could be said that this blurring started with other police reality shows such as COPS. It seems clear, at least in some instances, that officers behave differently when on camera. While this sometimes might result in more restrained behavior of the part of both the police and citizens, it can also result in behavior that veteran police officers see as 'pure and simple TV' but tactically flawed (Dittrich, 2007).[26]

Partnerships of this nature can result in unique problems and criticisms for the police agency that becomes involved in these shows. A variety of allegations have surfaced after one of the show's targets killed himself. A 56 year-old long time county prosecutor, Louis Conradt, Jr., is alleged to have communicated with a Perverted Justice decoy posing as 13 year-old boy in a Murphy Texas sting. These communications were sexually explicit and under Texas law constituted a felony even though Conradt never went to the target house. Warrants were obtained, and after police forcibly entered Conradt's residence, he shot himself in the head and died. Resulting criticisms of the operation include allegations that the investigation was botched (the search warrant had the wrong date and county for service), that sexual predators were actually drawn to the community by the sting, and that the arrest was rushed in order to allow NBC to get the arrest on tape (McCollum, 2007). It is noteworthy that local prosecutors originally declined to assist with the show, saying they were not involved in 'show business.' Even more interesting is the fact that charges on the twenty-three men arrested during the sting were not pursued when the district attorney ultimately found that "the Murphy Police Department was merely a player in the show and had no real law enforcement position. Other people are doing the work, and the police are just there like potted plants, to make the scenery" (Dittrich, 2007).

Police agencies should explore the motivation behind those with whom they partner and should carefully check the background of those who assist them. If, as in the case of Perverted Justice, they are being paid for their participation, careful thought should be given to how that will impact the legality of any arrests and the public perception. Prior to engaging in operations with others, the agencies should liaison with appropriate prosecuting authorities and heed their advice and warnings. To do otherwise invites failure and second

[26] In the Murphy, Texas Dateline sting, a veteran SWAT officer who was working off duty to provide security at the undercover house observed questionable tactics in the takedowns of the suspects, particularly the drawn guns and potential cross-fire situations and intensity of the takedowns. The article notes: "All that business—the guns, the tackling, the shouting—struck Detective Patterson as pure and simple TV: It might look good on camera, but if you're letting a camera influence how you do your takedowns, you've got a problem."

guessing. An operations plan should be prepared detailing the duties and responsibilities of all parties. During operations the CEO must ensure constant supervision to avoid the tendency to take shortcuts. Periodic updates should be required and an after action report should be prepared to critique the operation.

UNIVERSITIES

Other, perhaps less controversial, sources that policing should liaison more frequently with in the future are universities and colleges. Forensic computing degrees are being offered by a number of institutions. Forensic computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable (McKemmish, 1999). Partnering with a university that offers a degree in computer forensics offers a number of benefits. The University of Tulsa (TU) provides assistance to the Tulsa Police Department, the Oklahoma State Bureau of Investigation, and the Secret Service. Members of these agencies are provided workspace in the Tulsa Digital Forensics Laboratory on the University campus to allow them to work together on cyber criminals. The lab, funded by grants, has advanced computers and more space than the agencies are able to provide. In addition, twenty TU students a year intern and assist the law enforcement agencies in investigations (Marciszewski, 2005).

The University Police Department (UPD) at California Polytechnic State University was the driving force behind the creation of a high tech resource group which includes local law enforcement from 5 counties, state agencies, the FBI, the district attorney's office, and private corporations. The group provides high tech training to the members and share expertise in high tech crime investigation. The forensic expertise of the university officers and the support and assistance of the faculty and staff has resulted in the successful conclusion of numerous investigations (Aeilts, 2005).

In addition to the immediate benefits of assistance with investigations and training, partnerships with academic institutions can also result in fertile recruiting ground for the agency interested in recruiting personnel with computer/technological expertise. An agency with a reputation for being technologically friendly and advanced is much more attractive to recruits than one with a traditional view of policing.

INFRAGARD

Agencies should consider joining Infragard, a program of the Federal Bureau of Investigation, started in 1996. Infragard is an association of businesses, academic institutions, state and local law enforcement, and others dedicated to sharing information and intelligence about potential hostile acts against the country. Of the top 100 firms in the Fortune 500, 83 have an Infragard representative. The group initially was directed toward cyber-infrastructure protection but after the terrorist attacks of 9/11, the emphasis was broadened to include both physical and cyber threats to critical infrastructure. Local chapters hold regular meetings to discuss issues,

potential threats, and other issues that impact their industries. Local chapters provide training, local newsletters, and contingency plans in the event of attacks on the information infrastructure. (Infragard, 2007). The networking opportunities available with this group can be beneficial to both large and small agencies.

CONCLUSION

As in most areas of policing, partnering with others can be of assistance in addressing cybercrime. It is critical that CEOs of police agencies not be seduced by the quick fix (as we are too often in policing) and that any partnership and operations be consistent with the agencies vision, mission and values. Careful planning and proper supervision can help in addressing the pitfalls.

Strategies for local agencies to combat cybercrime:

*establish liaison with local universities or colleges which have resources

*identify local/regional/state/federal resources that can assist them as needed

*identify personnel within the agency who have computer expertise

*recruit new employees with the needed skills

*train personnel in cyber crime and computer related crime

*identify companies/private entities which have the skills, equipment, and desire to assist the agency with cybercrime investigations.

*have directives in place to ensure computer evidence is legally, properly seized

*keep abreast of the threat. Some ways to do this include joining Infragard and reading the annual CSI/FBI Computer Crime and Security Survey.

References

Aeilts, T. (2005). Defending against cybercrime and terrorism: A new role for universities. *FBI Law Enforcement Bulletin*, *74*(1), 14-20.

Commission on Accreditation for Law Enforcement Agencies. (2006). *Standards for law enforcement agencies: The standards manual of the law enforcement agency accreditation program* (5th ed.). Fairfax, VA: Author.

Dittrich, L. (2007). Tonight on Dateline this man will die. *Esquire.* Retrieved September 23, 2007, from http://www.esquire.com/features/predator0907#story.

Ellis, M. (2004). Mom's sleuthing helped find missing daughter. *The Columbian*. Retrieved September 23, 2007, from http://www.genderberg.com/phpNuke/modules.php?name=News&file=article&sid=98.

Futuristics & Law Enforcement. (2000). *The Millennium Conference*. Retrieved September 30, 2006, from http://www.fbi.gov/hq/td/fwg/conference.htm.

Infragard. (n.d.). *Infragard.* Retrieved September 26, 2007, from http://www.Infragard.net/about_us_facts.htm.

Marciszewski, A. (2005, May 1). Students provide know-how for cops. *Tulsa World*, A19.

McCollum, D. (2007). The shame game: “To catch a predator” is propping up NBC’s Dateline but at what cost? *Columbia Journalism Review*. Retrieved September 23, 2007, from http://www.cjr.org/feature/the_shame_game.php.

McKemmish, R. (1999). *What is forensic computing?* Canberra, Australia: Australian Institute of Criminology. Retrieved September 30, 2006, from http://www.aic.gov.au/publications/tandi/ti118.pdf.

Perverted Justice. (n.d.). *The PeeJ guide: For parents and first-time visitors to Perverted-Justice.com*. Retrieved September 30, 2006, from http://www.perverted-justice.com/guide/.