Community Policing in Cyberspace

by Art Bowker,
Cybercrime Specialist

Today's law enforcement administrator is well acquainted with community policing. We all know it involves being proactive and increased community interaction. Traditionally the focus has been on the "brick and mortar" world. This approach neglects the increasing significance of cyberspace to one's community. Unfortunately,whatsometimesstartsoutincyberspaceendsupinour communities. Law enforcement should therefore consider making cyberspace a part of their community policing efforts.

Some in law enforcement may argue that cyberspace is not under their jurisdiction and therefore not their concern. Shipley and Siebert (2008) have effectively countered this argument. They note that frequently crime fighting efforts are centered on: where are the victims, where are the suspects, where did the suspects/victims meet, and/or where did the crime occur? If a law enforcement agency can answer "their jurisdiction" when dealing with cybercrime, it quickly becomes apparent that there is a need to expand their community policing efforts.

The next argument centers on the extent of that expansion. Most police departments have some type of website presence. At a basic level these websites provide contact information about the department. Some may provide a method for filing complaints. However, just like a modern police building does not reflect a department's community policing efforts; neither does the best website represent a true community policing presence in cyberspace. At the other end of the spectrum: Is law enforcement being actively involved in prevention of cybercrimes? This is the approach is articulated as follows:

"In the physical neighborhood the crime prevention program promotes the use of better locks, better lighting, marking property with traceable identifiers, keeping a watchful eye out for neighbors, and what people should do if they fall victim to a crime. Community policing in the virtual neighborhood works to meet many of these same goals. In the case of the Internet, the members of the community are users of systems making a connection to the Internet. For each system connected, there is an owner and system administrator that represents a potential victim of a cybercrime. These potential victims need to partnership with law enforcement to identify problems that lead to cybercrime and to develop methods to mitigate their risk to the threats and prevent cybercrime." (SANS)

This approach is one of the hallmarks of the FBI's InfraGard programs and the Secret Service's Electronic Crime Task Forces (ECTF). InfraGard

" ... is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States."

The ETCF " ... network is to bring together not only federal, state and local law enforcement, but also prosecutors, private industry and academia. The common purpose is the prevention, detection, mitigation and aggressive investigation of attacks on the nation's financial and critical infrastructures."

Unfortunately, many local police department's lack the staff, resources and/or the expertise for this type of cyberspace policing, which focuses on protecting computers, data, and our infrastructure. Local police departments however can adopt a cyberspace presence that is meaningful to their communities. To determine that presence let's consider what community policing involves. Bennett and Hess define community policing as:

> " ... *an organization-wide philosophy and management approach that promotes: 1) community, government and police partnerships; 2) proactive problem solving to prevent crimes; and 3) community engagements to address the causes of crime, fear of crime and other community issues." (Bennett and Hess, 2007, p. 65)*

In keeping with this definition, local law enforcement should first become cyberspace partners. As noted above, two good partnerships that have developed are the InfraGard and the ECTF. Another such organization is the High Technology Crime Investigation Association (HTCIA). HTCIA is the largest non-profit professional organization in the world devoted to the prevention, investigation, and prosecution of crimes involving advanced technologies. Its members are made up of law enforcement and private sector individuals involved in cyberspace investigations. It focuses not only on networking between its members but also training. One of the largest HTCIA chapters is located in Ohio (ohiohtica.org). Becoming a partner with one or more of these organizations will help a local law enforcement agency develop valuable networks with others involved in investigating and protecting cyberspace.

There are also problem-solving approaches to prevent cybercrimes that impact local communities beyond the well-known undercover operations to apprehend Internet predators. One example is local police can develop law enforcement profiles for social networking sites, such as MySpace. Youth can be encouraged to list these law enforcement profiles as a "friend" on their own pages. Imagine the chilling effect on a predator locating a promising target, only to discover a police officer listed as a "friend." Police can also routinely check popular networking sites for profiles reported in their community. Checking these profiles can alert police to developing gang activity or problems in the school. Many local schools are activity involved in this "policing" of cyberspace to detect violations of school regulations. Developing school partners can further assist law enforcement efforts in this regard.

Another way to police cyberspace is to utilize information in the Ohio eSORN system. Recent changes to sex offender registration require sex offenders to disclose "any email addresses, Internet identifiers, or telephone numbers." (O.R.C. 2950.041 and 2950.05) Law enforcement can check on such information pertaining to local sex offenders and do Internet searches to determine if this information is appearing in cyberspace areas that pose a risk to the community. Examples might be personal ads or new profiles on social networking sites. Some offenders obviously may not disclose Internet identifiers or e-mails in their sex offender registration. However, some of these same offenders will reuse, reactivate, or slightly modify old identifiers or e-mails. Searches of old identifiers may reveal sex offenders violating sex offender registration law and posing an obvious risk to the community.

"There are ... problem-solving approaches to prevent cybercrimes that impact local communities beyond the well-known undercover operations to apprehend Internet predators. One example is local police can develop law enforcement profiles for social networking sites, such as MySpace."

Community engagement can occur through cyberspace safety presentations to local schools, businesses, retirement communities, etc. Such presentations can help educate community residents regarding the dangers lurking in cyberspace and how to prevent one's self from becoming a victim. They also provide a method to announce law enforcement initiates, such as the police profiles mentioned earlier.

Making law enforcement a visible force in cyberspace can only benefit our communities. However, just like police need bulletproof vests in the real community, they also need to be protected in cyberspace. Law enforcement should make sure such their initiatives are properly secured with up-to-date antivirus software as well as a firewall. Additionally, police need to be aware that evidence collected in cyberspace, such as a troubling profile, needs to be collected in a legally defensive manner. (Shipley, 2008) SEARCH has excellent training materials for law enforcement starting out cyberspace, such as "How to Capture a MySpace Page for Investigative Purposes." Again, consultation with other cyberspace partners such as InfraGard, the ECTF, and HTCIA will help prepare law enforcement to extend community policing to cyberspace in a safe and secure manner.

The Internet has made our world a lot smaller. Law enforcement at all levels must be prepared to address the challenges that may come up as a result. Making cyberspace a part of an agency's total community policing efforts will help address those challenges that may appear in our local communities. ■

References:

Bennett, W. W & Hess, K. M. (2007). Management and Supervision in Law Enforcement.
Califorinia: Thompson Wadworth
Community Policing on the Internet. Retrived January 29, 2009, SANS from
https://www.sans.org/reading_room/whitepapers/awareness/community_policing_on_the_internet_917
Daniels,K. & Wagner, L. (2008). How to Capture a MySpace Page for Investiative Purposes. SEARCH (search.org)
Infragard, Retrieved January 29, 2009, from http://www.infragard.net/
High Technology Crime Investigation Association, Retrieved January 29, 2009, from http://htcia.org
Electronic Crimes Task Forces, Retrieved January 29, 2009, from http://www.ustreas.gov/usss/ectf.shtml
Ohio Chapter of HTCIA, Retrieved January 29, 2009, from http://ohiohtcia.org
Ohio Revised Code 2950.041, Retrieved January 29, 2009, from http://codes.ohio.gov/orc/2950.041
Ohio Revised Code 2950.05, Retrieved January 29, 2009, from http://codes.ohio.gov/orc/2950.05
Shipley, T. (2007), Collecting Legally Defensible Online Evidence: Creating a Standard Framework for Internet Foresnic Investigations. Vere Software (http://www.veresoftware.com)
Shipley, T. & Silbert, W. (2008) Online Investigation Best Practices presented at 2008 National Symposium on Cyber Crime, U.S. Pretrial Services, Southern District of California

About the author: Art Bowker has been employed in law enforcement and corrections for almost 24 years. He currently is the cybercrime specialist for the U.S. Pretrial Services and Probation Office for the Northern District of Ohio. In 2008, he was the international president of the High Technology Crime Investigation Association (HTCIA). HTCIA is the largest nonprofit professional organization of its kind in the world. Bowker has written numerous articles which have appeared in the FBI Law Enforcement Bulletin and Federal Probation on cybercrime, cybersex offenders, financial and criminal history investigations. He has a Master's of Arts degree in corrections and a Bachelor's of Science degree in criminal justice studies from Kent State University.