Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Community Policing on the Internet

Community policing has been applied to the physical world with good success. These programs establish a community partnership that attempts to solve the problems that lead to crime, and work to change these factors to mitigate the threat of crime. One of the main cruxes of community policing is crime prevention. This paper applies the principles of community policing and crime prevention to the Internet and details establishing relationships between law enforcement and potential victims, their individual roles and resp...

Copyright SANS Institute
Author Retains Full Rights

AD

Community Policing on the Internet

ABSTRACT

The Internet is quickly becoming the world's largest electronic neighborhood. The ability to establish instant communication links between businesses, friends and enemies has shrunk the planet to a size that one could consider a neighborhood. This neighborhood has the potential to foster crime and other malicious activity more easily than its physical counterpart. Cybercrime is increasing and the victims are many times ill prepared to prevent the crime or deal with the aftermath, there needs to be proactive approach to crime prevention in the Information Age.

Community policing has been applied to the physical world with good success. These programs establish a community partnership that attempts to solve the problems that lead to crime, and work to change these factors to mitigate the threat of crime. One of the main cruxes of community policing is crime prevention. This paper applies the principles of community policing and crime prevention to the Internet and details establishing relationships between law enforcement and potential victims, their individual roles and responsibilities, and some of the problems the relationship may alleviate such as fears a victim may have concerning the reporting of cybercrime.

Introduction

In many places across the United States police work is returning to a practice that takes officers out of patrol cars and puts them on foot, bicycle or horse patrol. This return to placing officers back in the neighborhood and making them approachable by the people they serve is referred to as "Community Policing". Community policing attempts to establish a partnership between law enforcement and the community with a goal of solving neighborhood problems that may be promoting crime. Once the partnership has identified potential problems, the police seek to change the environment in an effort to mitigate their risks and deter crime. In most cases, a large portion of this change relies on crime prevention.[1] 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.

While it may seem elementary to most system administrators that there is a need for firewalls, intrusion detection, virus protection, and routine system patching, there are systems and networks that do not follow these best practices. Whether it's a lack of

[1] About Community Policing

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

funding for security or neglected systems, the failure to adhere to best practices poses a great deal of risk to the rest of the Internet. Civil liability for such practices may be the only deterrent for such negligence, but that's another topic altogether. Community Policing on the Internet is a proactive crime prevention approach that establishes relationships with potential cybercrime victims, fosters information sharing, and overcomes the fears normally associated with reporting cybercrime.

Identifying Members of the Community

Potential victims of threats on the Internet today include anyone with an Internet connection. Is it possible for Community Policing program to encompass such a large constituency? No. Just as real world Community Policing programs focus on one neighborhood, the same holds true for Community Policing on the Internet. While the Internet is global, there exists logical divisions or boundaries by the type of business or geographic location. In identifying potential victims, one of these boundaries needs to be selected. From there, law enforcement can approach various user groups or business organizations and establish a dialogue on cyber crime issues. Whether this occurs through presentations to user groups or booths at local trade shows, law enforcement must begin to foster better relationships with potential cybercrime victims.

When discussing cybercrime the goal of the law enforcement agency should convey several key points:

- Law Enforcement realizes that cybercrime is a real threat[2]
- Demonstrate the need for firewalls, IDS, and AVP
- Explain how most fears concerning reporting cybercrime are not valid
- Explain the benefits to reporting cybercrime
- Explain how to report a cybercrime
- Explain how information on incidents may be shared anonymously for the benefit of others in the community
- Demonstrate the need for formal incident response procedures

The Threat of Cybercrime

Statistics on the number of computer systems present on the Internet has continued grow over the last several years and constitute a large potential victim pool.

[2] Selgado, Richard. Working With Victims of Computer Network Hacks

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[3]

The potential victims encompass every level of user from novice to expert. The cost of computer crime for victims continues to rise. According to the Computer Security Institute (CSI) / Federal Bureau of Investigation (FBI) survey "Computer Security Issues & Trends" for 2001, total annual losses due to computer crime rose from $100,119,555 in 1997 to $377,828,700 in 2001.[4] Attorney General John Ashcroft estimates losses from cybercrime in America to be in the billions of dollars each year.[5]

The U.S. Office of Attorney General has responded to the cybercrime treat by increasing the amount of training related to cybercrime provided to US Attorneys. A Special Computer and Telecommunications Crime Coordinator is now located in each federal judicial district. The FBI has responded to the cybercrime threat by creating over 16 computer crime units in metropolitan areas around the country.[6] The FBI has recently started hiring more computer specialists, created a new cyber division, begun developing more computer forensics labs, and increased the number of computer hacking and intellectual property units.[7]

The FBI also acts as the coordinating authority for the National Infrastructure Protection Center (NIPC), which promotes a private and public partnership with three core initiatives to address the protection of critical infrastructures that if lost or damaged "would have a debilitating impact on the defense or economic security of the United States."[8]

---

[3] Internet Software Consortium
[4] Power, Richard. Computer Security Issues & Trends (CSI/FBI) p. 11
[5] Ashcroft, John. Remarks of Attorney General John Ashcroft
[6] Ibid.
[7] Matthews, William. FBI Seeks Help vs. Cybercrime
[8] NIPC - Frequently Asked Questions

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

NIPC Core Initiatives[9]

- Infragard - A community based organization to bring together private sector critical infrastructure entities and the government to promote information sharing
- Warnings – Providing Infragard members with information concerning critical infrastructure protection through Advisories, Alerts, and Warnings.
- Analysis – Providing analytic products based on information from intelligence, law enforcement, and private sector communities

In addition to efforts at the federal level, many states are gearing up to perform forensic analysis on computer systems associated with computer crime and are developing statutes that deal directly with computer crime instead of making traditional crimes fit the cybercrime mold.[10]

The federal government is not the only one trying to get a handle on cyber crime. A March 2001 study "Electronic Crime Needs Assessment for State and Local Law Enforcement" by the U.S. Department of Justice (USDOJ) Office of Justice Programs lists the "Critical Ten" needs for state and local law enforcement:[11]

1. Public awareness
2. Data and reporting
3. Uniform training and certification courses
4. Onsite management assistance for electronic crime units and task forces
5. Updated Laws
6. Cooperation with the high-tech industry
7. Special research and publications
8. Management awareness and support
9. Investigative and forensic tools
10. Structuring a computer crime unit

The results of this study clearly illustrate the needs of state and local law enforcement related to cyber crime deterrence, laws, and investigation. Many of the needs follow the principles of community policing and are being met by many state and local governments.

As a community based organization, Infragard is law enforcement's attempt to define a community and work with the constituents as part of what may be called a community policing effort. Just as in the real world, the community-policing endeavor in the digital realm strives to meet the same goals. [12]

[9] NIPC Pamphlet
[10] Stambaugh, Hollis, et. Al. Electronic Crime Needs Assessment for State and Local Law Enforcement
[11] Ibid.
[12] Flynn, Mary Kathleen. Safety in Numbers

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Goals of Community Policing[13]

- Community Partnership
- Problem Solving
- Change Management

The community partnership is established by first identifying the community, providing a means of communication through an Infragard initiative or other common traits held by members of the community and leveraging the partnership to address the problems faced by the constituency to make changes that are beneficial to all parties. These changes might include providing awareness training to members of the community concerning threats and ways to mitigate them. Just as the crime prevention officer goes out to community centers and civic groups to explain the proper methods of securing homes against break-ins, the cyber crime prevention officer needs to be able to go out and spread the word on the latest threats to information systems and how these threats may be mitigated. While law enforcement officers cannot be expected to provide information security consulting services, they should be a relevant and constant source of threat information and offer referrals to technical documents detailing the risk and abatement procedures. Dialogue with potential victims provides other opportunities for fostering beneficial relationships by putting names with faces in the law enforcement community prior to an incident where the victim needs the law enforcement assistance.[14] The relationship between law enforcement and potential victims may also foster more information sharing on incidents, but until all of the fears of cyber crime reporting are quelled cyber crime reporting may continue to be a problem.

The Case for Reporting Incidents and Sharing Information

Cyber crime victims have several fears and misunderstandings associated with reporting the crime. Richard Selgado with the Department of Justice lists several in his publication "Working with Victims of Computer Network Hacks"[15], as does the article Fear Factor in the October 15th, 2002 issue of CIO Magazine.[16]

A expanded list of fears, myths and misunderstandings from these publications are:

- Victim is unaware of the computer crime laws that might apply to an incident
  - What is a computer crime?
  - Statutory Jurisdiction
    - Local
    - State
    - Federal
- Victim is unsure of which agency to call
  - Investigative Jurisdiction
- Fear everyone will find out - Bad Publicity
  - Disclosure of intellectual property

[13] About Community Policing
[14] Flynn, Mary Kathleen. Safety in Numbers
[15] Selgado, Richard. Working with Victims of Computer Network Hacks
[16] Scalet, Sarah D. Fear Factor

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

  - Loss of investor confidence
  - Freedom of Information Act (FOIA)
  - Sunshine Laws and Public Records Statutes
- Fear that law enforcement will not act or there will be no value to the victim for reporting the incident
  - Monetary damage thresholds prevent investigation and prosecution
  - Report taken, but case never worked
  - Determination that offender is a juvenile or located in another jurisdiction that will not cooperate with the investigation
  - Government determines the case does not merit prosecution
- Fear that law enforcement will come in and shutdown operations during the investigation
  - Seizure of computers
  - Downtime during initial investigation & evidence collection
  - Loss of employee due to time to prepare and testify in court
- Fear that law enforcement will not have the expertise to investigate the crime

While these fears are real, they can be overcome by awareness campaigns on the part of law enforcement that illustrate their willingness to be a partner in addressing the bigger problem of cyber crime instead of only looking for the successful arrest and prosecution of the perpetrators.[17] Ultimately successful investigation and prosecution may prove to be a much needed deterrent to cyber crime but going into an investigation with arrest and prosecution as the only goal does not benefit the victim or law enforcement. The approach taken by law enforcement today has to address the need for gather information on incidents and how this need to understand cyber crime and share the information with other potential victims can sometimes outweigh the perceived benefit of prosecution. Attorney General John Ashcroft supports reporting and sees reporting as one method that may help to stop repeat attacks.[18] FBI Director Robert Mueller estimates that his agency is only receiving about one-third of the reports that he would like to get. He says this prevents the FBI from doing its job. Mueller admits that he understands the fears held by victims alluding to bad publicity and disclosure of intellectual property.[19]

Many of the fears associated with reporting cyber crime can be overcome by establishing a relationship with law enforcement officers prior to an incident.[20] These relationships allow the potential victim to ask questions concerning their fears and get answers. Richard Segado states:

> "Most of the industry participants thought that law enforcement investigators would remove the servers, proceed without any victim input, that it would disrupt the normal operations of the company for weeks at a time, and that law enforcement's involvement would mean

[17] Ibid.
[18] Ashcroft, John. Remarks of Attorney John Ashcroft
[19] Matthews, William. FBI seeks help vs. cybercrime
[20] Selgado, Richard. Working with Victims of Computer Network Hacks

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

> that the company could not take steps to secure the system or conduct its own investigation."[21]

Given the opportunity, law enforcement officers can explain how they have handled past investigations, the outcomes, and where these fears of reporting are unfounded. Law enforcement officers need to reassure the potential victim that business data will be handled in confidence and seizure of critical assets will usually not be an issue. These pre-established relationships can also serve as a means to convey the basics of reporting cyber crimes by providing procedures on when and how to report an incident.[22] Law enforcement may also want to cover their investigative capabilities and explain that, in many cases, they will require the assistance of the system administrators during the investigation.

Federal agencies may soon fall under new security guidelines, which will provide them with a list of vendors who are authorized by the GSA to conduct security assessments. The results of these assessments are then used to determine if the agency meets required information security levels based on the sensitivity of the information they process. While governments can regulate information security, much of the private sector is self-regulated. What's secure to one business may be considered open to another. The problem with mitigating risk and deterring cyber crime for those whose systems are open is an enormous problem for law enforcement officials and the Internet. Just as a crime prevention officer will visit a home or business and evaluate physical security, the same service is not available for information security. While the police can't offer information security vulnerability assessments they can offer information on forming an incident response plan, a top 20 list of vulnerabilities,[23] and a means for to initiate a dialogue concerning cyber crime threats and responses.

The other services that law enforcement can provide that benefit both the victim and the law enforcement agency are incident reporting forms that gather the basic facts of the case and give the victim a starting point for incident response. One reporting form is presently available on the NIPC website (http://www.nipc.gov/incident/cirr.htm). This form is not an acceptable means to convey classified information and should not be used when such information must be included in the report. Another shortcoming of this web based reporting method is the lack of encryption through SSL. A portable document format is available for download and should be considered a safer alternative until SSL is implemented on the report page. Another source of reporting forms is the CIO Cyberthreat Response and Reporting Guidelines from CIO magazine.[24] In addition to a basic reporting form, this document includes lists of federal, state, and local agencies as well as other reporting bodies and resources for cyberthreats. The includes a

[21] Ibid.
[22] CIO Cyberthreat Response & Reporting Guidelines
[23] SANS Institute. Twenty Most Critical Internet Security Vulnerabilities
[24] CIO Cyberthreat Response & Reporting Guidelines

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

detailed listing of all FBI and United States Secret Service field offices in the United States.

On the information sharing front, many industries such as banking and finance have taken the initiative to form their own Information Sharing and Analysis Centers (ISAC) to provide a means to share information in a timely manner so that risk and attack information can be quickly disseminated to other members for mitigation and response.[25]

Other industry specific ISAC's include:[26]

Electric	www.nerc.com
IT	www.it-isac.org
Oil & Gas	www.energyisac.com
Telecom	www.ncs.gov
	www.ncs.gov/Image-Files/ISAC_Fact.pdf
U.S. Government	www.fedcirc.gov
Water	www.amwa.net/isac/

For some, membership in an ISAC may pose as much risk as releasing proprietary information or potentially damaging information through reporting cyber crime to law enforcement. The FS-ISAC addresses these concerns by allowing the member to sanitize the information before it is submitted and subsequent automated and human review of the data before it is shared with other members.[27] While the ISAC doesn't directly involve law enforcement, a recent agreement between the NIPC and the Financial Services ISAC (http://www.fsisac.com) allows them (FS-ISAC) to talk to the NIPC on a weekly basis.[28]

In sharing information with the government there remains the one question begging to be answered. How will public records laws such as the Freedom of Information Act (FOIA) protect or require disclosure of confidential data? The existing B4 exemption provides protection for "trade secrets and commercial or financial information" and many in government feel this exemption is adequate protection, but both the Senate and House included an additional FOIA exemptions in their versions of the bill to create the new Department of Homeland Defense.[29] The enacted legislation retained the House version of the FIOIA exemption, which provides more protection of the entity and the information shared from disclosure.[30] Many feel this exemption is too broad and may result in the ability of corporations to hide misdoings that involve critical infrastructures. The bill's provision to exempt voluntarily shared information from disclosure covers information "related to the security of critical

[25] Flynn, Mary Kathleen. Safety In Numbers
[26] CIO Cyberthreat Response & Reporting Guidelines
[27] Scalet, Sarah D. Fear Factor
[28] Ibid.
[29] Fear Factor Sidebar – Fact, Fiction and FOIA
[30] Matthews, William. Bill's Secrecy Provisions Stick

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

infrastructure or protected systems."[31] Information shared with the Homeland Defense Department cannot be used in civil suits and any government employee who provides leaks the information may be prosecuted criminally. Some believe the protection mechanism also extends to information held by State government's thus overriding any state laws that normally require the records to be open to the public.[32] Further complaints about the FOIA exemption the law criticize the ability of the government to use the shared information in regulatory matters while the information is still not part of the public record.[33] The debate over exemptions to the 36-year-old FOIA is sure to continue, but the latest exemption does seem to limit liability while providing a means for corporations to provide information to the government that may help secure national critical infrastructures.

Conclusion

The community policing initiative on the Internet is logical starting point for crime prevention efforts and community awareness of the threats facing the digital domain. The telecommunication industry and its users are quickly realizing, in the wake of 9/11, that a fiber optic cable can be just as important as the electricity feed into their buildings from the local power company. However, even knowing the potential for disruption of service from various cyberthreats, many people continue to run open networks with little regard for security. And the major problem may not be hackers and virus makers, but the system administrators who are provided patches to apply and fail to do so before disaster strikes. If the community policing and awareness initiative can make a real change concerning the perception information security of these system administrators, it will be worth the effort. Corporations will continue to be hesitant about reporting cybercrime, but the ability to do so in confidence with the new protections afforded to them by homeland security legislation, may help alleviate some of their fears. While the government wants people to come forward and report the crimes and support prosecution so the sentences of the perpetrators can be used as a deterrent for other would be hackers, the government must realize that most protections afforded by various FOIA exemptions are not protections in the courtroom when evidence is presented. Law enforcement and criminal justice officials must remain cognizant of the limitations of the FOIA exemptions and put the needs of the victim, to protect themselves, above the perceived need for prosecution when necessary. Community policing partnerships require some flexibility and the ability to keep an open dialogue between the members of the community and law enforcement. Without open communications between them, any community policing effort is subject to fail.

[31] Reaction to Passage of the Homeland Security Bill - OMB Watch
[32] Ibid.
[33] Ibid.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

1. "About Community Policing." URL: http://www.communitypolicing.org/about2.html (22 Oct. 2002)

2. Selgado, Richard. "Working with Victims of Computer Network Hacks." March 2001. URL: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_6.htm (7 Oct. 2002)

3. Internet Software Consortium "Internet Domain Survey Host Count." URL: http://www.isc.org/ds/hosts.html (10 Oct. 2002)

4. Power, Richard. "Computer Security Issues & Trends." Vol. VII, NO. 1. Spring 2001. Computer Security Institute & San Francisco Federal Bureau of Investigation Computer Intrusion Squad.

5. Ashcroft, John. "Remarks of Attorney General John Ashcroft @ First Annual Computer Privacy, Policy & Security Institute." 22 May 2001. URL: http://www.cybercrime.gov/AGCPPSI.htm) (29 Oct. 2002)

6. Matthews, William. "FBI Seeks Help vs. Cybercrime." Federal Computer Week. 1 Nov. 2002. URL: http://www.fcw.com/fcw/articles/2002/1028/web-fbi-11-01-02.asp (31 Dec. 2002)

7. National Infrastructure Protection Center (NIPC) "Leading the Government's Efforts To Protect Our Nation's Critical Infrastructure" Pamphlet.

8. Stambaugh, Hollis. Et. Al. "Electronic Crime Needs Assessment for State and Local Law Enforcement - NCJ 186276." March 2001. URL: http://www.ncjrs.org/pdffiles1/nij/186276.pdf) (30 Oct. 2002)

9. Flynn, Mary Kathleen. "Safety in Numbers" CSO Online (Nov. 2002) URL: www.csoonline.com/read/110802/safety.html) (15 Nov. 2002)

10. Scalet, Sarah D. "Fear Factor." CIO Magazine. 15 Oct. 2002. URL: www.cio.com/archive/101502/fear_content.html) (17 Nov. 2002)

11. "CIO Cyberthreat Reporting Guidelines." CIO. URL: http://www.cio.com/research/security/incident_response.pdf (17 Oct. 2002)

12. SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus." Version 3.21. 17 Oct. 2002. URL: http://www.sans.org/top20/ (31 Dec 2002)

13. Fear Factor Sidebar "Fact, Fiction and FOIA." 15 Oct. 2002. URL: http://www.cio.com/archive/101502/fear_sidebar_1.html (17 Oct 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

14. Matthews, William. "Bill's Secrecy Provisions Stick." Federal Computer Week. 19 Nov 2002 URL: http://www.fcw.com/fcw/articles/2002/1118/web-foia-11-19-02.asp (31 Dec 2002)

15. "Reaction to Passage of Homeland Security Bill." OMB Watch 20 Nov. 2002 URL: http://www.ombwatch.org/article/view/1194/1/138/ (31 Dec. 2002)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced