GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Crime and Punishment:
The Psychology of Hacking in the New Millennium

© SANS Institute 2004, Author retains full rights.

Cynthia Fitch, M.Ed
GSEC Practical Requirements (v.1.4b)
Dec. 26, 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Crime and Punishment:
The Psychology of Hacking in the New Millennium

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

In order to effectively combat computer crime and discourage hacking activity, lawmakers and computer professionals must understand the motivation behind this activity. The hacking community is a diverse and complicated universe, comprised of multiple skill layers and motivations. By understanding the different types of hackers and what motivates their behavior, it is possible to profile computer crime, making it easier to predict future activity. If the best offense is a good defense, then the best way to predict potential hacking attempts is to understand the mentality of hackers. One way of understanding the hacking mentality is by examining research based on social psychology theory. Though other fields use psychological profiling to help solve crimes like serial killings and terrorism, there have only been a few studies done connecting psychological theory with computer crime. This research, while very in-depth, can be distilled down to a few basic principals: social learning via peer groups and justification of illegal activity. This paper will discuss the different subcultures in the hacking community, the different motivations of the various subgroups and a simple explanation of the research involving the social learning theory and computer crime, in order to explain this behavior.

Origins of Hacking in the American Conscious

Computer crime and hacking have been forged into the American conscious by the mass media, and have spawned numerous stereotypes that have been sustained throughout the past two decades. Through popular movies and books, the media has created a surreal image of computer crime and hackers that is more often than not more fiction than reality. Yet the term “hacker” has a relatively benign etymology. In the 1950’s and 1960’s, the computer world revolved around the mainframe environment. Since personal computers did not exist at that time, programmers had to make the most of their access to the mainframe computer. A ‘hack’ referred to a fast work around, or shortcut that was undertaken to improve a program or to yield faster results. Hacking was not yet a derogatory term, but rather a compliment associated with exploration, experimentation and learning. Around the same time, as the computer world

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

moved from a mainframe environment to networked systems, phone phreaking, which involved manipulation of telephone networks, began to attract the interest of many of the same technologically minded people in the computer field. Over time, people would utilize both hacking and phreaking skills in order to explore remote systems and share information. Devitt states, "not until the early 1980s did the word "hacker" earn disdain, when people like Kevin Mitnick, Kevin Poulsen and Vladimir Levin began using computers and the Internet for their own questionable gains."[1]

Categories of Hacking

Hacking has evolved over the years to include many different motivations and activities. Unfortunately, hackers are still perceived and portrayed as one uniform group with a single purpose. The media portrays anyone who engages in illegal computer activity as a "hacker," without investigating or considering their motivations and goals. Today, the term hacker has become "generic and refers to a rather diverse community (i.e., crackers, coders, script kiddies, programmers, criminals, etc.)."[2] By and large, most researchers have created their own hierarchy of hackers. While most researchers have created their own naming convention for the various categories of hackers, most have consistently identified the same common subgroups.[3]

Categories: MacAfee defines two major categories: Black Hats and White Hats. Others have since added Gray Hats. Thomas takes that notion one step further and adds Gray Hats, for those hackers in between. He notes that all hackers break into systems by definition, but what separates the Black Hats from the White Hats and Gray Hats is intent.

White Hats: A White Hat usually works within the laws of the hacker ethic (to do no harm)[4] or as a security expert. Most hackers that define themselves as White Hats are interested in improving security of computer systems, operating systems, software and networks. Young and Aitel note:

> They see the need to protect the public by actively discovering security holes in software and making the public aware of this issue. White Hats

---

[1] Michael Devitt. "A Brief History of Computer Hacking." *Available from* http://www.chiroweb.com/archives/19/13/04.html

[2] Marcus Rogers. "A New Hacker Taxonomy," page 1. *Available from* http://www.cerias.purdue.edu/homes/mkr/

[3] These have been summarized in interest of space. Specific scales have been attributed to their authors.

[4] Steven Levy. *Hackers: Heroes of the Computer Revolution* (Anchor Press/Doubleday: Garden City, 1984).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

> work together with the vendors of particular software to solve the issue and make the digital world more secure. Even if the vendor takes several months to fix the hole, the White Hat would not publish the information before the vendor does.[5]

Curry notes that White Hats "have a long tradition of trying to improve the computing community and its resources. They look for weaknesses and vulnerabilities with the intent of making knowledge public in order to improve the quality of services and products."[6]

Black Hats: The self-perception of a Black Hat is that they force software vendors and system administrators to fix security problems by publishing known vulnerabilities. Bischoff concludes that the main motivator of the Black Hat is power. "Once they (Black Hat) realize what kind of power they hold, they eventually begin to rationalize and start to believe that what they're doing is OK."[7] Black Hats are associated with anger and hate, whether against a specific company or country, and are often associated with web defacements.[8] Black Hats have no qualms about stealing or destroying data on the networks that they penetrate.

Gray Hats: The term "Gray Hat" was originally coined by the L0pht--one of the best-known old-school hacking groups…for those who wanted to stand apart from corporate security testers but also distance themselves from the notorious Black Hats. The category defined by this phrase has come to encompass most independent security experts and consultants, as well as many corporate security researchers."[9] Gray Hats are usually "reformed Black Hats now working as security consultants, or hackers who mix consulting with fraudulent access."[10] There is controversy surrounding the Gray Hats. Some experts feel that any group that creates hacking tools, despite their intent, are not ethical. "As far as I'm concerned, an ethical problem would exist in people doing security work that

---

[5] Susan Young and Dave Aitel. *The Hacker's Handbook: The Strategy behind Breaking into and Defending Networks* (Auerbach Publications: Boca Raton, 2004), 34.

[6] Sam Curry. "Bug Watch: Hacker Motivation," 11 October 2002, p. 2. Available from http://www.vnunet.com/news/1128187

[7] Glenn Bischoff. *"Fear of a Black Hat," Telephony.online* (Sept 3, 2001) Available from http://telephonyonline.com/microsites/magazinearticle.asp?mode=print&magazinearticleid=117383&releaseid=&srid=11357&magazineid=7&siteid=3

[8] MacAfee column, Esecurity News "Who are hackers: Where do they come from and why are they called hackers?" (January 2002). Available from http://dispatch.mcafee.com/esecuritynews/jan2002/firewallforum.asp

[9] Robert Lemos. "New Laws Making Hacking a Black and White Choice" *CNET News* (Sept 23, 2002) http://news.com.com/2009-1001_3-958129.html

[10] Darren Thomas. *Art of War, Part3, (*Aug 2003), p. 2 Available from http://www.infosecnews.com/opinion/2003/08/06_01.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

are also releasing tools useful to hackers, and if that's the case, its l0pht's [sic] problem, not ours," one CEO told AntiOnline.[11]

Classes: There are various classes of hackers under both the Black Hat and White Hat categories. The following is the most commonly cited types of hacker classes:

- *Elite*- The hackers who have both the knowledge and skills of the highest level. This is the rarest type of hacker, having experience, skill and ethical integrity. The elite tend to be White Hats that understand the network infrastructure and have programming skills that allow them to write their own tools. It is generally agreed upon that elite hackers do not engage in criminal activity or harbor malicious intent but rather expose security flaws and other coding problems. Most elite hackers alert system administrators to security issues, rather than publish vulnerabilities.[12] Elite status can also be gained by a particularly famous exploit or hack, or mere longevity on the scene.[13]

- *Script kiddies* - the most scorned subgroup within the larger hacker community. These tend to be the youngest, least skilled hackers, who use exploit tools created by the elite hackers.[14] They might undertake known exploits and scans for unpatched systems, but they don't have skills to find such problems or write tools to exploit them.[15] Script kiddies aren't motivated by any particular factor, but rather seek out easy targets. When the media mentions a "hacker" attack, they are usually referring to a web defacement or Denial of Service (DOS) attack perpetrated by a script kiddie. Public perception of hacking is largely shaped by this subgroup's actions. Verton sites Mafiaboy as one of the more infamous script kiddies.[16]

- *Cyber-terrorists*. It's not just their potential to crash the net via a denial of service attack (or any other technique aimed at crippling internet communication and transmission of data). Rather it's the anonymity that the net offers them for exchanging information and sharing plots online.

---

[11] Jeff Andrews. "Glorifying Gray Hats," Available from http://www.netsys.com/firewalls/firewalls-2000-02/msg00357.html

[12] Jeremy Quittner. "Hacker Psych 101" Available from http://tlc.discovery.com/convergence/hackers/articles/psych_print.html

[13] Winn Schwartau. *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption* (Thunder's Mouth Press: New York, 2000) 39.

[14] Ron Hale. *Intrusion Crackdown* Available from http://www.itsecurity.com/papers/telenisus.htm

[15] Kim Zetter. "Hacker Nation," *PC World* (May 2001), 4.

[16] Dan Verton. *The Hacker Diaries: Confessions of Teenage Hackers.* (McGraw-Hill/ Osborne: New York, 2002), 83.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

By using stenography and cryptology, cyber terrorists can cloak information in plain sight, making it hard for anyone not specifically scanning for such techniques, and easy for any of their comrades, to find. Due to international strife, cyber-terrorists are poised to become the most serious of computer criminals. Some countries use the Internet as a training and recruitment tool, while others use the 'net for information gathering. Nation-state hacking can also be included in this category, as it focuses on information warfare and governmental spying.[17]

- *Disgruntled (ex) employees*—one of the most dangerous, least publicized groups. These corporate insiders have specific information regarding practices and policies of an organization, thus making it easier for them to circumvent security, gaining access for themselves or others.[18] Rogers' cites Post, who indicates that these hackers tend to be introverts with a sense of "entitlement combined with a narcissistic personality. These individuals believed they were owed special recognition by their organizations and would seek revenge if they did not receive it." [19]

- *Virus Writers*- Sarah Gordon, a virus expert, notes that the virus subculture is not homogenous, and that while they share methodologies with hackers, the two groups have developed along different paths.[20] Virus writers tend to exploit weakness found by hackers, who then code methods to execute those flaws.

- *Hactivist*- This name derives from blending the words "activism" and "hacking".[21] One of the fastest growing hacker subgroups, hactivists deface websites and launch DOS attacks to satisfy political, religious or social agendas. Curry notes that the agenda hackers are will stop at nothing until they achieve their political goal or effect economic duress on the victim for their cause.[22] These actives are motivated to wreck havoc rather than to learn more about systems or software vulnerabilities. This subgroup's motives can be closely tied to that of the cyber terrorists.

Problems with Taxonomy

There are critics of the aforementioned classifications. Spafford states "hats are obvious, behavior isn't. And what is white to one person may be gray to

---

[17] Young and Aitel, 36.
[18] Ron Hale, *Intrusion Crackdown* Available from http://www.itsecurity.com/papers/telenisus.htm
[19] Rogers, "Taxonomy," 6.
[20] Gordon, Sarah. "Viruses in the Information Age". *Available from* *http://www.badguys.org/vb3part.htm*
[21] Young and Aitel, 35.
[22] Curry, Sam. "Bug Watch: Hacker Motivation," 2.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

another."[23] Most of the research has come from self-reported surveys and other types of documents that depend on the person in question being honest. Since the field of hacking is a meritocracy, where one's status comes from his/her reputed skills and exploits, it is reasonable to believe that some of the self reported data, especially concerning individual class level and hat, might be inflated or wrong.[24] The line between White Hat and Black Hat is a perception for most hackers, many of who might not agree about what constitutes illegal behavior. Hats are a matter of self-definition, and with so many hackers having a loose grip on legalities, their take on whether they are legitimate or not seems suspect. For example, Deth Veggie, a veteran member of the hacking group Cult of the Dead Cow (cDc), states that "just because something is illegal doesn't mean it's wrong."[25] Mayur Kamat goes even further, comparing hackers to history's greatest minds. "Galileo, Pythagoras, etc had been banned because of the knowledge they possessed which was contradictory to popular belief. Same [sic] is the case with hackers. They possess that knowledge which others don't want them to possess."[26] This type of moral reasoning sheds light on the problem of hacker logic and moral equivocalness. Most citizens would consider something that is illegal to be wrong, thus making hacker perceptions of whether they are white or Black Hat suspect at best.

Stereotypes and Myths

The lack of a formalized taxonomy also creates the opportunity for the stereotyping of hackers. Hackers are one of the most stereotyped groups in modern American, due in large part to the movies produced in the last two decades. Thomas asserts that popular culture is the biggest reason for the mythical image of hackers. "Movies like *War Games, The Net, Hackers* (complete with the tagline "their only crime is curiosity") and *Sneakers* all have heavily influenced perceptions of hackers, both in the popular imagination and to hackers themselves."[27] The popular image of hackers as alienated, angsty teens who live isolated lives chained to their P.C.'s is not valid, according to Dan Verton. Verton's research on several different teenage hackers illustrates that they come from a diverse background and engage in a variety of "normal" activities, including sports. While most of the subjects of Verton's book are hackers or engaged in hacking activity, none of them are isolated, alienated youth. Most of the teens profiled in the book are normal kids, muddling through everyday life issues.[28]

---

[23] *SC Infosec Opinionwire* Dec. 11, 2002, p.1 Available from http://www.infosecnews.com/opinion/2002/12/11_01.htm

[24] http://seti23.org/wiki.pl?HacKer

[25] Kim Zetter, 4.

[26] Mayur Kamat. "Hacking" Oct. 27, 2003. Available from http://www.boloji.com/computing/security/005.htm

[27] Douglas Thomas. "Hacker Stereotypes: The Glass Menagerie" *USC Online Journalism Review* (Oct, 28, 2003) p2. http://www.ojr.org/ojr/business/1017969669.php

[28] Verton, 187.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Yet the popular media seizes on the Mafiaboy's of the world, and creates work after work of fiction based on this stereotypical disaffected teen model. And while most hackers learn as teens, the common traits they share are a fascination with technology, desire to learn, and interest in "figuring" out a network. It is the challenge these kids share, not the Def Con uniform of leather and body piercing. These are the same motivations that carry most teenage hackers through to their adult years, where their motivations remain the same: curiosity, control, intellectual challenge, and prestige.[29] The media, however, is more concerned with a quick sound byte, then actually educating the American public about the different between script kiddies and hactivists. Young and Aitel state, "…the media has changed its view on "hackers," constructing a more nefarious image, which can of course be better used for exciting news, reports, and articles. But the image is still a stereotype."[30]

Yet these stereotypes of hacking have taken hold of the American conscious and become ingrained as fact in the American mind. Aiding the misconception of hacking and computer crime is the absolute dearth of empirical research data on the subject. In the current world climate, with security foremost on most computer professionals' minds, research into the motivations of hackers is essential into predicting behavior and understanding their reasons for engaging in such computer crime.

Research

Criminology is one of the few academic or professional groups that have attempted to research hackers and classify their behavior into systematic models of behavior based on theory. Though few studies exist, the prevailing theory and school of thought that has best described computer crime in general, and hackers in particular, is the social learning theory. The social learning theory is concerned with the relationship between social and environmental factors and their influence on behavior. According to Rice, humans "learn by observing the behavior of others and by imitating this pattern—a process referred to as modeling."[31] Modeling is based on the assumption that behavior is often patterned after the observed habits of others. Humans naturally observe the actions of others and if those actions are successful (i.e. bring rewards or other positive reinforcements), then others will attempt that same behavior. However, if a particular action brings sanctions or punishment (i.e. negative reinforcements), then those observing will tend to avoid that behavior. This theory has strong implications for peer groups, as humans tend to copy or imitate the modeled successful strategies while ignoring those choices that are

[29] John Collins. "Illegal Internet" from http://www.design-ireland.net/hack/contents.php
[30] Young and Aitel, 31.
[31] Phillip Rice. *The Adolescent: Development, Relationships, and Culture*, 8th ed. (Allyn and Bacon: Boston, 1999), 43.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

unsuccessful. As long as a group member follows acceptable behavior, social learning works to implant positive behavior in the rest of the group.

The Social Learning Theory

The Social Learning Theory is based on the idea that crime is a learned behavior. Leighninger states that "people learn criminal behavior through the groups with which they associate. If a person associates with more groups that define criminal behavior as more acceptable than groups that define criminal behavior as unacceptable, the person will probably engage in criminal behavior."[32] Put another way, "just as people must learn though socialization how to conform to their society's norms, they must also learn how to depart from those norms. Therefore, deviance, like conforming behavior, is a product of socialization"[33] This theory shows how a juvenile can socially learn deviant behavior from those around him/her such as family, peers, schoolmates or anyone else that he or she may come in contact with. Parents and peers are the most powerful agents in socialization.

Virtual Peer Groups

Despite stereotypes of hackers being alienated loners, hackers are surprisingly social in nature. While most computing activity might take place alone, most hackers form social circles where information is exchanged and connections are made. Since hacking is a meritocracy, information is something to be bartered. The expertise needed to be a hacker is so diverse that no one can attempt to know everything about it. Therefore, one's expertise is something that can be bartered or exchanged for programs, utilities or even more knowledge. Though some of this interaction is in person, face to face, such as Def Con and 2600 meetings, most social interaction takes place in the virtual world.[34] The computer revolution has changed peer groups to an extent: no longer are they identifiable by association in some physical location, but rather defined by same goals and interests in cyberspace, in Internet Relay Chat (IRC) and message boards. These virtual groups allow hackers a forum to exchange knowledge, brag about their supposed exploits and skills, and to trade tools and information.[35] Script kiddies are particularly known for this type of bravado.[36] Verton attributed Mafiaboy's chat room bragging as part of the information that led investigators to

---

[32] L. Leighninger & Phillip R Popple. *Social Work, Social Welfare, and American Society*, 3rd. ed. (Allyn and Bacon: Needham Height, 1996), 331.

[33] Calhoun, C., Light, D., & Keller, S. *Sociology*, 5th. ed. (Alfred A. Knopf: New York, 1989), 176.

[34] Rogers, "Taxonomy," 9.

[35] Young and Aitel, 32.

[36] ibid, 33.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

his door.[37] Young and Aitel state that "today's script kiddies spend most of their time in IRC" and that they have "an internal social structure" trained in exchanging information in a short time.[38]

Elite hackers tend to associate on a more personal basis. Groups like cDc (Cult of the Dead Cow) and L0pht are hacker groups that have been in existence for many decades and worked together closely in that time. Their social patterns mimic more traditional, rather than virtual peer groups.

Other avenues of hacker's social interaction include the Def Con convention and mass market publications like *2600*. Both serve as avenues of communication, information sharing and social interaction.

Therefore, hacking social circles and peer groups take on an increased importance. Not only do they serve as place for the exchange of information and building of reputations, but they also increase the chances that a person will be exposed to and thus engage in criminal behavior. Skinner and Fream research found that there was a positive correlation between peer group involvement in computer crime and an individuals' tendency to engage in illegal computer activity.[39]One of the best works dealing with computer crime and the social learning theory is Marcus Rogers' thesis on the social learning theory, moral disengagement and computer crime.[40]

Moral Disengagement

One aspect of the social learning theory that Rogers' inspects is moral disengagement. Moral disengagement is the use of neutralizing definitions to justify behavior than an individual knows is wrong. In other words, hackers justify their illegal activity with excuses in order to avoid feeling bad about it. Hackers use moral disengagement as a method to avoid or reduce guilt associated with 'bad' or illegal behavior.[41]

Peer groups are important to this process of moral disengagement, because if a person is surrounded by people who constantly dehumanize the victim or justify hacking into systems, then that person's moral center shifts, and they begin to accept that illegal behavior is justified. Rogers states "self censure can be disengaged or weakened by stripping the victim of human attributes, or shifting the blame onto the victim…Blaming the victim or circumstances allows the

[37] Verton, 67.
[38] Young and Aitel, 32.
[39] W. Skinner & A. Fream. A Social Learning Theory Analysis of Computer Crime Among College Students, *Journal of Research in Crime and Delinquency,* 1997.
[40] Rogers, Marcus. *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study,* 2001. Doctoral Dissertation, University of Manitoba, Canada.
[41] Ibid.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

perpetrators to view themselves as victims who were provoked. The perpetrator's actions now become construed as defensive. The victims are blamed and accused of bringing the actions upon themselves."[42] An example of this behavior in the hacker community would be blaming a system administrator for failing to secure his system, thus justifying the hacker's illegal entry into the system. If the system's administrator is to blame for not doing his job, then the hacker has justified his actions and removed guilt for breaking the law. Hacker's also tend to use moral disengagement when they blame software vendors for writing bad code, or not providing fixes to known flaws fast enough. Rogers also notes that "their activities are purely an intellectual activity and that information should be freely available to every."[43] All of these excuses are examples of moral disengagement. Peer groups are vital to the process of moral disengagement because an individual hacker or a novice hacker views the norms of the group and in turns adopt those same beliefs. This reinforces and justifies illegal behavior, thus fulfilling the social learning theory and ensuring that hacking activity thrives.

One of the problems with social theory being applied to computer crime and hacking is that there are only a few research projects that have studied the problem. Social psychology has also been blamed for its lack of empirical data, though researchers have worked out ways to measure the theory in regards to research practices. Another issue with studying the hacking community is that most all the data we have has been self-reported, thus subject to the honesty of the individual hacker. As stated earlier, most hackers build their reputations within their peer groups by bragging about their exploits. These attribute of the population, along with all the inherent flaws of self reported data, casts doubt of the validity of the research.

Another issue is the recent development of peer to peer file sharing. While Hollinger's research of computer crime among college students indicates that only 10% of all students engaged in crime (defined as password cracking, access to systems without permission, and software copying), recent studies have indicated that file sharing is a near epidemic among the college population. One poll suggested that nearly 69% of college students say they download music, yet only 2 % report actually paying for those downloads.[44] Most students use moral disengagement to justify their non-payment, by citing the cost of overpriced compact discs in regards to the cost to produce them. Yet Hollinger's (and most other research) does not include this relative recent development in technology. All these issues illustrate that new, more in-depth research needs to take place, in order to get a better understanding of the hacker community.

[42] Ibid., 40.
[43] Ibid., 46.
[44] "P2P Makes a Dent," *Computer Power User* (December 2003), 12.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Mitigating Illegal Activity

While hacking activity and other computer crime might never be vanquished, there are steps that can be taken to minimize the growth of it. The social learning theory illustrates that individuals are influenced by the behavior of their peers. When there are no perceived penalties associated with illegal computer activity, hacking activity increases. Therefore, there is a need to highlight the consequences of engaging in hacking activities. While law enforcement is struggling with ways to effectively track and prosecute computer criminals, there needs to be an emphasis put on publicizing those who are caught and convicted of computer crime. Many petty offenders are caught, but the outcomes of their trials are not made that public. Meanwhile, major offenders either are not convicted (Knight Lightning AKA Craig Neidorf) or are convicted then released to great fanfare and adulation (Kevin Mitnick).[45] Parker (1998) sites that some hackers are eventually rewarded for their illegal activity by the use of the positive reinforcements, such as a high paying job in the security industry. Many hackers such as Mitnick have gone on to form their own security company, while also playing the role of media darling for the press. Meanwhile, Parker argues that there are few negative reinforcements, as few hackers are caught, prosecuted, or sentenced to jail time.[46] The research shows that computer crime increases when the perception of hackers is that there will be no retribution. This needs to change in order to affect change.

Education is another key in limiting the growth of hacking. Many researchers cite the need for teaching kids and computer professionals alike the ethics of computer use, including copyrights, and the laws surrounding what is legal and illegal activity.[47] There is a need for schools and other institutions to incorporate the ethical use of computer resources into daily life. Whether this is assigning papers on copyright infringement or illustrating the misuse of resources, an effort needs to be made to actively teach our citizens what behavior is illegal, as well as ethically wrong.

The media needs to find ways of deemphasizing the "cool" factor of hacking. This is not a call for censorship, but rather a call for a more balanced view of hacking, to illustrate that certain types of activity are illegal for a reason, and that computer crimes do have victims. The Motion Picture Association of America has managed to appeal to the public using clips that feature what impact pirating DVD's has on the average movie industry worker. By showing the faces of

---

[45] Bruce Sterling. *The Hacker Crackdown*. (Bantam: New York, 1992), 239.

[46] D. Park. *Fighting Computer Crime: A New Framework for Protecting Information.* (John Wiley & Sons: New York, 1998).

[47] Denning, Dorothy. "Hacker Ethics." Available from http://www.southernct.edu/organizations/rccs/resources/research/security/denning02/teaching_comp_ethics.html#teaching

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

regular people (and not stars who make millions of dollars a year), the MPAA is fighting moral disengagement by showing that decreasing profits affects the jobs of regular people. Unlike the RIAA, that has moved from one publicity nightmare to another, the M.P.A.A.'s campaign elicits empathy and not anger, yet manages to focus on the morality of not pirating. This is a good first step and this model should be emulated by other corporations seeking to limit their profit loss.

There should also be outlets for the genuine curiosity that exists among young computer enthusiasts. There needs to be an emphasis put on creating hacking competitions and other sites that encourage this intellectual interest, while creating a controlled atmosphere created specifically for this purpose. While these do exist, there needs to be more effort to recruit young people. By providing an outlet for curiosity and a place to learn new skills and exercising existing ones, a perfect mentoring environment can be created. Computer experts could use this as an opportunity to groom the next generation of security experts, while subtly exerting positive regard for laws, copyrights, and the fine line between curiosity and breaking the law. Mentoring kids who show an interest in the field, rather than slapping them with jail terms and fines, can far influence behavior better than any law could hope to.

Conclusion

In the century of the existence of the automobile, it took nearly 100 years for seatbelt laws and drunk driving intolerance to prevail. We live in a time when technology is outpacing society's moral adaptability. Within time, balance will be restored and what is in societies best interests will emerge and triumph. We live in an age of moral ambiguity, where there is little consensus about what behavior is right or wrong, and what constitutes illegal behavior.

The computer revolution has brought many changes to our daily lives outside of the business world. The rapid growth of the personal computer has far outpaced our society's ability to adapt, leaving a morally ambiguous area surrounding what is "right" and "wrong" and what is "legal" and "illegal". The judicial system and law enforcement are also mired in this ambiguity, making it difficult for the public to understand what constitutes illegal behavior. Parents can't ingrain ethics into their children when they most likely don't know how to operate their own home computer. Educating both parents and children is a priority, so that any grey areas are fully explained and people can make fully informed decisions about their behavior and computer activities. While hacking attempts are growing and computer crime becoming more prevalent, defining behavior as deviant (i.e. creating more laws) is not always the best answer. The spread of malicious viruses and worms is a threat to both the home user and the business environment. However, creating new laws that add to the ineffective existing laws is not the answer. We must strive to change behavior and attitudes. And in order to do that, we must better understand hackers.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

Andrews, Jeff. "Glorifying Gray Hats," Available from http://www.netsys.com/firewalls/firewalls-2000-02/msg00357.html

Bischoff, Glenn. "*Fear of a Black Hat," Telephony.online* (Sept 3, 2001) Available from http://telephonyonline.com/microsites/magazinearticle.asp?mode=print&magazinearticleid=117383&releaseid=&srid=11357&magazineid=7&siteid=3

Calhoun, C., Light, D., & Keller, S. *Sociology*, 5th. ed. (Alfred A. Knopf: New York, 1989).

Collins, John. "Illegal Internet" from http://www.design-ireland.net/hack/contents.php

Curry, Sam. "Bug Watch: Hacker Motivation," 11 October 2002. Available from http://www.vnunet.com/news/1128187

Denning, Dorothy E. "Hacker Ethics." Available from http://www.southernct.edu/organizations/rccs/resources/research/security/denning02/teaching_comp_ethics.html#teaching

Devitt, Michael. "A Brief History of Computer Hacking." Available from http://www.chiroweb.com/archives/19/13/04.html

Gordon, Sarah. "Viruses in the Information Age". Available from *http://www.badguys.org/vb3part.htm*

Hale, Ron. *Intrusion Crackdown* from the website http://www.itsecurity.com/papers/telenisus.htm

Leighninger, L., & Popple, Phillip R. *Social Work, Social Welfare, and American Society,* 3rd. ed. (Allyn and Bacon: Needham Height, 1996).

Lemos, Robert. "New Laws Making Hacking a Black and White Choice" *CNET News* (Sept 23, 2002) http://news.com.com/2009-1001_3-958129.html

Levy, Steven. *Hackers: Heroes of the Computer Revolution* (Anchor Press/Doubleday: Garden City, 1984).

MacAfee column, Esecurity News "Who are hackers: Where do they come from and why are they called hackers?" (January 2002). Available from http://dispatch.mcafee.com/esecuritynews/jan2002/firewallforum.asp

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Park, D. *Fighting Computer Crime: A New Framework for Protecting Information.* (John Wiley & Sons: New York, 1998).

"P2P Makes a Dent," *Computer Power User* (December 2003).

Quittner, Jeremy. "Hacker Psych 101" Available from website http://tlc.discovery.com/convergence/hackers/articles/psych_print.html

Rice, Phillip, *The Adolescent: Development, Relationships, and Culture*, 8th ed. (Allyn and Bacon: Boston, 1999).

Rogers, Marcus. *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study,* 2001. Doctoral Dissertation, University of Manitoba, Canada. Available from http://www.cerias.purdue.edu/homes/mkr/

Rogers, Marcus. "A New Hacker Taxonomy," *Available from* http://www.cerias.purdue.edu/homes/mkr/

SC Infosec Opinionwire Dec. 11, 2002. Available from http://www.infosecnews.com/opinion/2002/12/11_01.htm

Schwartau, Winn. *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption* (Thunder's Mouth Press: New York, 2000).

W. Skinner & A. Fream. A Social Learning Theory Analysis of Computer Crime Among College Students, *Journal of Research in Crime and Delinquency,* 1997.

Bruce Sterling. *The Hacker Crackdown*. (Bantam: New York, 1992).

Thomas, Darren. *Art of War, Part3, (*Aug 2003). Available from http://www.infosecnews.com/opinion/2003/08/06_01.htm

Verton, Dan. *The Hacker Diaries: Confessions of Teenage Hackers.* (McGraw-Hill/ Osborne: New York, 2002).

Young, Susan and Aitel, Dave. *The Hacker's Handbook: The Strategy behind Breaking into and Defending Networks* (Auerbach Publications: Boca Raton, 2004).

Zetter, Kim. "Hacker Nation," *PC World* (May 2001).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.