WWW.Criminologia.org

TELEMATIC JOURNAL OF CLINICAL CRIMINOLOGY

Telematic Journal of Clinical Criminology - www.criminologia.org International Crime Analysis Association

Anno di pubblicazione 1999

Modern-day Robin Hood or Moral Disengagement

by Marc Rogers, M.A,. 1999

Understanding the Justification for Criminal Computer Activity

The rapid growth of information technology has introduced a new category of criminal offender, the computer criminal (Denning, 1998; Parker, 1998; Rasch, 1996; Rogers, 1999; Taylor, 1997). Computer criminals often mistakenly referred to as "hackers" have defended their actions as being ethical and attempt to justify their behavior in terms of serving some higher moral function (Chandler, 1996; Chantler, 1997; Denning, 1998; Parker, 1998; Spafford, 1997). Some computer criminals subscribe to the notion of the ends justifying the means (Chantler, 1996). These individuals assume that the "ends" of their activities are ethical therefore their activities are ethical (Chantler, 1996). This is an interesting and somewhat convoluted line of reasoning and assumes that one can truly know and understand all the consequences of one's actions. This is extremely hard if not impossible, especially in an immature area such as the Internet and computer technology (Spafford, 1997).

Spafford (1997) argued that the activity of hackers should be evaluated not in terms of the ends, or the justifications, but by the acts themselves. Although Spafford (1997) may be correct, the justifications and rationalizations of individuals engaging in aberrant behavior can provide insight into the psychological mechanisms being employed (Bandura, 1990). The purpose of this thesis is to present a psychological foundation for understanding the computer criminal's rationalization and justification of his or her aberrant behavior.

The second half of the twentieth century has become known as the "Information Revolution" (United Nations, 1999). Information technology now touches almost every aspect of life and has become the backbone for telecommunications, finance, governments, health care, and education (Gattiker & Kelly, 1997; Littman, 1997; Rapalus, 1997; United Nations, 1999). Entire infrastructures have been built to support information technology (i.e., high-speed network backbones, fiber optics, etc.) and advances in information technology such as the Internet have effectively erased economic borders and introduced the concept of the "Global Community" (Flohr, 1995; United Nations, 1999).

The Information Revolution has also has brought with it some unique social, moral, and legal problems. As with other advances, the staggering growth of information technology has outpaced society's ability to govern, and possibly understand its implications (Denning, 1998; Howard, 1997; Mizrach, 1997; Parker, 1998; Power, 1996; United Nations, 1999). The growth rate of the Internet alone is staggering. In July of 1999 it was estimated that there were approximately 60 million host computers attached to the Internet, it has been predicted that by the year 2000 there will be over 200 million host computers attached (ISC, 1999). It has also been estimated that by the year 2000 the revenue in North America from electronic business (e-business) will be in the billions of dollars (Weil, 1999).

The world of information technology is unique, in that it is without borders, and to date there is no clear delineation of jurisdiction (Davis & Hutchison, 1998; Rasch, 1996; United Nations, 1999). Information technology has opened the doors for the dissemination of information and the sharing of ideas (Denning, 1998; Rogers, 1999). However, a certain negative element has arisen that is using information technology for vandalism, fraudulent activity, espionage,

terrorism, revenge, perversion, and other criminal activities (Adamski, 1999; Clarke, 1998; Denning, 1998; Kanrow et al., 1994; Mizrach, 1997; Rapalus, 1997; Schwartau, 1997).
With society's increasing dependence on computer systems the consequences of computer crimes can be extremely grave. To date there have been documented attacks against emergency 911 systems, air traffic control systems, stock exchanges, railways, banks, military, and private businesses (Denning, 1998; Parker, 1998; United Nations, 1999). The most recent US figures indicate that in 1998-99, computer crimes cost US businesses a minimum of $126 Million USD (Power, 1999).
Due to the potential for harm, computer crimes and computer criminals are attracting the attention of governments, law enforcement, and many international bodies such as the United Nations (Clarke, 1998; United Nations, 1999). These organizations are struggling with the nuances of dealing with both the individuals involved and the political fallout from their activities (i.e., extradition treaties, international definitions of crime, etc.).
In today's society computer criminals have been mistakenly referred to by the media as "hackers". The term hacker was not originally saddled with a negative connotation (Levy, 1985). The term at one time was a complement and referred to an innovative programmer such as those at Massachusetts Institute of Technology (MIT) or Stanford University who could figure out novel methods to overcome obstacles (Gattiker & Kelley, 1997; Chandler, 1996; Sterling, 1992). However, today the term hacker has become synonymous with criminal computer related activities and as Hafner & Markoff (1995) suggested "cyber-punks".
Individuals who are engaging in illegal computer activity have developed a certain mystique (Chantler, 1996; Denning, 1998; Parker, 1998; Rogers, 1999). They are commonly portrayed by themselves and the media as modern-day "Robin Hoods", who are performing a valued function for society (Chantler, 1996; Parker, 1998; Rogers, 1999). There have been numerous articles, editorials, interviews, and web pages that state that without hackers there would be no or very ineffective information security (Spafford, 1997; Taylor, 1997; Rogers, 1999). Interviewed hackers contend that they are the watchdogs, keeping a vigilant eye on the unscrupulous vendors and tyrannical governments (Taylor, 1997). Publications such a phrack and 2600 commonly carry editorials justifying the sometimes illegal activity of hackers, and urging other individuals to join the cause.
Certain portions of society are accepting at face value, the justifications being offered by these computer criminals (Parker, 1998; Rogers, 1999). To the younger generation some computer criminals are becoming role models (e.g., Kevin Mitnick). This has led to a variety of "copy-cat" and/or "one-upmanship attacks", a trend, which is quite disturbing. The media has also contributed to the problem by mistakenly associating the term "hacker" with computer criminals (Chantler, 1996; Taylor, 1997). As mentioned previously the original definition of hacker had little or anything to do with criminal activity (Levy, 1985). The term "hacker" does not have the same negative connotations that "criminal" does, and as such it is useful when attempting to justify or make more palatable, certain behaviors (Bandura, 1990; Rogers, 1999).
The fact that computer criminals need to justify their aberrant behavior in terms of fulfilling some higher societal need, can be understood in the context of social cognitive theory and the psychological concept of moral disengagement (Bandura, 1990; Bandura et al., 1996; Rogers, 199). Social cognitive theory attempts to explain how individuals who are engaged in aberrant behavior justify their activities (Bandura, 1990; Bandura et al., 1996;). According to the theory, people tend to refrain from behaving in ways that violate their moral standards (Bandura et al., 1996). Moral reasoning is translated into actions through what Bandura termed self-regulatory mechanisms, through which moral agency is exercised (Bandura et al., 1996). In other words, people refrain from behaving in a manner that violates their moral standards because this behavior would bring self-censure (Bandura, 1990; Bandura et al., 1996).
Moral agency consists of a self-regulatory system that operates through three major subfunctions (Bandura, 1990; Bandura et al., 1996). The subfunctions are: self-monitoring, judgmental, and self-reactive (Bandura, 1990; Bandura et al., 1996). The first step to exercising control over one's conduct is self-monitoring. Actions give rise to self-reactions

through a judgmental function in which the individual's conduct is evaluated against their internal standards and situational circumstances (Bandura, 1990; Bandura et al., 1996).
The theory states that there are four major points in the self-regulatory system at which internal moral control can be separated from detrimental conduct (Bandura, 1990; Bandura et al., 1996). An individual can disengage self-sanctions by re-construing the conduct, obscuring the personal causal agency, misrepresenting or disregarding the negative consequences of the action, vilifying the victims, and maltreating them by blaming and devaluing them (Bandura et al., 1996; Bandura, 1990).
People do not usually engage in reprehensible conduct unless they have justified to themselves the rightness of their actions (Bandura et al., 1996). The process of moral justification allows for the detrimental conduct to be made personally and socially acceptable by portraying it in the service of valued social or moral purposes (Bandura et. al., 1996; Bandura, 1990).
According to the theory, language plays an important role in shaping an individual's perception of his or her actions (Bandura et. al., 1996; Bandura, 1990). Reprehensible conduct can be masked by euphemistic language and, in some cases, it can allow the conduct to be seen as respectable (Bandura, 1990; Bandura et al., 1996). The individual can be relieved of a sense of personal agency by convoluted verbiage (Bandura, 1990; Bandura et al., 1996). Reprehensible conduct can also be masked by comparison to other more injurious behavior (Bandura, 1990; Bandura et al., 1996). The advantageous or palliative comparison is more effective when more flagrant activities are used in the comparison (e.g., comparing embezzling money from a large corporation to the poisoning of the environment by multinational corporations) (Bandura, 1990; Bandura et al., 1996).
Another set of dissociative practices operates by distorting the relationship between the agent's actions and the effects of the actions (Bandura, 1990; Bandura et al., 1996). With displacement of responsibility, individuals view their actions as arising from social pressures and are, therefore, not responsible for their actions (Bandura, 1990; Bandura et al., 1996). Self-censure is reduced because the individual is no longer an actual agent of their actions (Bandura, 1990; Bandura et al., 1996). The action can also be ascribed to compelling circumstances and therefore not a personal decision (Bandura, 1990; Bandura et al., 1996).
Personal agency can also be obscured by diffusion of responsibility (Bandura, 1990; Bandura et al., 1996). This can occur by segmentation of duties, where each segment by itself is fairly benign, although the totality is harmful. Group decisions can also be used to diffuse the responsibility (Bandura, 1990; Bandura et al., 1996). Self-censure can be minimized by disregarding or distorting the consequences of an action (Bandura, 1990; Bandura et al., 1996). Ignoring the detrimental consequences of the actions, as in selective inattention or through cognitive distortion, reduces the feelings of guilt (Bandura, 1990; Bandura et al., 1996). The last set of disengagement practices focuses on the recipients of the acts. Self-censure can be disengaged or weakened by stripping the victim of human attributes (Bandura, 1990; Bandura et al., 1996). Dehumanization results in the victim being viewed as sub-human, and not as a person with feelings (Bandura, 1990; Bandura et al., 1996).
Blaming the victim or circumstances is another effective method that decreases self-censure (Bandura, 1990; Bandura et al., 1996). In moral disengagement by attribution of blame, perpetrators view themselves as victims who were provoked. The perpetrator's actions now become construed as defensive (Bandura, 1990; Bandura et al., 1996). The victim gets blamed and accused of bringing the actions upon themselves.
Using the moral disengagement as a foundation one can hypothesize that hackers and computer criminals are employing moral disengagement mechanisms in an attempt to reduce self-censure (Chantler, 1996; Denning, 1998; Parker, 1998; Rogers, 1999). Several studies and articles, quote hackers as stating that their activities are purely an intellectual activity, and that information should be freely available to everyone (Chantler, 1996; Taylor, 1997). Individuals engaged in criminal computer activity routinely minimize or misconstrue the consequences (Chantler, 1996; Denning, 1998; Parker, 1998; Post, 1996; Shaw et. al, 1998). These individuals have stated that they never intentionally damage any files, and that besides companies have or should have backups of their data and systems (Chantler, 1996). Other individuals dehumanize the victim and refer to them in terms such as multi-national

corporations, or just networks and systems. They usually do not comment on the impact to the end users and system administrators, the cost to potential consumers, or the long term effects (Littman, 1995; Parker, 1998; Spafford, 1997).
The attribution of blame to the victim is possibly the most common mechanism employed by computer criminals and hackers (Parker, 1998; Rogers; 1999; Taylor, 1997). The majority of research which have used interviews, and self-report surveys, quote the hacker subjects as blaming the system administrators or programmers for lax security, and stating the victims deserved to be attacked (Chantler, 1996; Parker, 1998).
It is probable that the justifications offered by the computer criminals for engaging in criminal activities is in fact moral disengagement (Rogers, 1999). The interviews, articles, web sites, and studies of computer criminals provide examples of all the concepts discussed by Bandura (1990). It is arguable that computer criminals despite their appeals to the contrary, are aware of the fact that what they are doing is not socially or perhaps morally acceptable. In order to reduce the self-sanctions and feelings of guilt that arise from engaging in aberrant behavior, the criminals have developed this "Robin Hood" persona. This persona, while popular with the often naive and manipulated media, does not stand up well to scrutiny and has been unsuccessfully attempted by other criminals such as terrorists, and white-collar criminals (Bandura, 1990).
The debate over the ethics of certain hacker activities will continue to be a contentious issue and will obviously not be solved by this thesis. The purpose of this thesis was to provide a possible psychological explanation for the observed tendency within the computer criminal community of portraying their illegal activities as beneficial to society

References

Adamski, A. (1999). Crimes related to the computer network. Threats and opportunities: A criminological perspective. Available: http://www.infowar.com/new.
Bandura, A. (1990). Mechanisms of moral disengagement. In Reich (Eds.). Origins of Terrorism; Psychologies, Ideologies, Theologies, Sates of Mind. (pp. 161-191). New York: Cambridge University Press.
Bandura, A. (1990). Selective activation and disengagement of moral control. Journal of Social Issues, 46, 27-46.
Bandura, A., Barbaranelli, C., Caprara, G., & Pastorelli, C. (1996). Mechanisms of moral disengagement in the exercise of moral agency. Journal of Personality and Social Psychology, 71, 364-374.
Chandler, A. (1996). The changing definition and image of hackers in popular discourse. International Journal of the Sociology of Law, 24, 229-251.
Chantler, N. (1996). Profile of a computer hacker. Florida: Infowar.
Clarke, R. (1998). Technological aspects of internet crime prevention. Available: http://www.anu.edu.au/people/Roger.Clarke/II/.
Davis, R., & Hutchison, S. (1998). Computer crime in canada. Toronto: Carswell.
Denning, D. (1998). Information Warfare and Security. Reading: Addison-Wesley.
Flohr, U. (1995). Bank robbers go electric. Available: http://www.byte.com/news.
Gattiker, U., & Kelley, H. (1997). Techno-crime and terror against tomorrow's organization: What about cyberpunks? Available: http://www.ncsa.com/library.
Hafner, K. & Markoff, J. (1995). Cyberpunks: Outlaws and hackers on the computer frontier. Toronto: Simon and Schuster.
Howard, J. (1997). Analysis of security incidents on the internet. Unpublished doctoral dissertation, Carnegie Mellon University, Pennsylvania.
Internet Software Consortium (ISC). (1999). Internet domain survey, July 1999. Available: http://www.isc.org.
Karnow, C., Landels, R. & Landels, D. (1994). Recombinant culture: Crime in the digital network. Avaliable: http://www.cpsr.org/privacy.
Levy, S. (1985). Hackers. New York: Dell
Littman, J. (1997). The Watchman: The twisted life and
crimes of serial hacker kevin poulsen. Toronto: Little Brown & Company.

Littman, J. (1995). The fugitive game: online with kevin mitnick. Toronto: Little Brown & Company.
Mizrach, S. (1997). Is there a hacker ethic for the 90s? Available: http://www.infowar.com.
Parker, D. (1998). Fighting computer crime: A new framework for protecting information. New York: John Wiley & Sons, Inc.
Post, J. (1996). The dangerous information system insider: Psychological perspectives. Available: http://www.infowar.com
Power, R. (1996). Testimony before the permanent
subcommittee on investigations. Available: http://www.gocsi.com/preleas2.
Power, R. (1998). Current and future danger. Computer Security Institute.
Power, R. (1999). CSI/FBI 1999 computer security survey. Computer Security Institute.
Rapalus, P. (1997). 1997 Computer crime and security survey. Available HTTP: Hostname: gocsi Directory: preleas.
Rasch, M. (1996). Criminal law and the internet. The
Internet and Business: A Lawyer's Guide to the Emerging Legal issues. Available: http://www.cla.org/RuhBook/chp11.htm
Rogers, M. (1999). Psychology of hackers: Steps toward a new taxonomy. Available: http://www.infowar.com
Schwartau, W. (1994). Information Warfare. New York: Thunder Mouth Press.
Shaw, E., Post, J., & Ruby, K. (1998). Information terrorism and the dangerous insider. Paper presented at the meeting of InfowarCon'98, Washington, DC.
Spafford, E. (1997). Are hacker break-ins ethical? In, Ermann, Williams, & Shauf, (Eds.) Computers, Ethics, and Society. (pp. 77-88). New York: Oxford.
Taylor, P. (1998). Hackers: the hawks and the doves-enemies & friends. Unpublished manuscript.
United Nations (1999). International review of criminal policy – United nations manual on the prevention and control of computer-related crime. Available: http:// www.ifs.univie.ac.at/~pr2gq1.
Weil, N. (1999). Survey says: T'is the season for online buying. Available: http://www.e-businessworld.com/idgns/1999/11/10/SurveySaysTisTheSeasonFor.shtml.