ABSTRACT

The means by which the U.S. justice system attempts to control illegal hacking are practiced under the assumption that hacking is like any other illegal crime. This chapter evaluates this assumption by comparing illegal hacking to shoplifting. Three inhibitors of two illegal behaviors are examined: informal sanction, punishment severity, and punishment certainty. A survey of 136 undergraduate students attending a university and 54 illegal hackers attending the DefCon conference in 2003 was conducted. The results show that both groups perceive a higher level of punishment severity but a lower level of informal sanction for hacking than for shoplifting. Our findings show that hackers perceive a lower level of punishment certainty for hacking than for shoplifting, but students perceive a higher level of punishment certainty for hacking than for shoplifting. The results add to the stream of information security research and provide significant implications for law makers and educators aiming to combat hacking.
INTRODUCTION

Interest in hacking has increased in popularity due to high-profile media coverage of system breaches. In June 2005, the information belonging to 40 million credit card holders was hacked through a credit card processor (Bradner, 2005). In 2006, about 18,000 personal records in the U.S. Department of Veterans’ Affairs had been compromised. A recent analysis of compromised electronic data records shows that about 1.9 billion records were reported compromised between 1980 and 2006. This means that for every U.S. adult, nine records have been compromised in aggregate. About 32% of the 1.9 billion compromised records were related to hackers (Erickson and Howard, 2007). Companies are reluctant to publicize that they have experienced information security breaches because of the negative impact such incidents have on their public image leading to loss of market value. Cavusoglu, Mishra and Raghunathan (2004) estimate the loss in market value for organizations to be 2.1% within two days of reporting an Internet security breach which represents an average loss of 1.65 billion.

The rise of computer and Internet use has coincided with an increase in ability of users to commit computer abuses (Parker, 2007) along with an increase in the number of unethical, yet attractive situations faced by computer users (Gattiker and Kelley, 1999). Recently, Freestone and Mitchell (2004) examined the Internet ethics of Generation Y. They found that hacking is considered less wrong than other illegal Internet activities such as “selling counterfeit goods over the Internet.” We recognize that illegal hacking activities encompass a wide array of violations of varying degrees of seriousness. For this study, we are not interested in any specific type of illegal hacking but rather illegal hacking activities in general.

Hacking is one of the technologically-enabled crimes (Parker, 2007). Originally the term hacker was a complimentary term that referred to the innovative programmers at MIT who wanted to explore mainframe computing and were motivated by intellectual curiosity and challenges (Chandler, 1996). However, the term became derogatory as computer intruders pursued purposefully destructive actions that caused serious damage for both corporations and individuals. American Heritage Dictionary (2000) defines a hacker as “one who uses programming skills to gain illegal access to a computer network or file”.

Hacking is a relatively new crime and, as such, is potentially perceived differently from other crimes. Most recently, there has been demand for research which will aid in developing an understanding of how computer crimes differ from more traditional crimes (Rogers, 2001). Due to cost-effectiveness concerns, the chief avenue utilized by the United States government to deter illegal behavior is to increase the severity of punishment (Kahan, 1997). This approach is also used to deter illegal hacking behavior. However, this approach to control illegal hacking is practiced with the assumption that the factors affecting illegal hacking are similar to the factors that influence other types of crime. We set out to evaluate this assumption by comparing illegal hacking activities to shoplifting. The decision to use shoplifting for comparison to illegal hacking was motivated by three reasons:

First, the act of shoplifting is in some ways similar to hacking in that both are acts of illegally obtaining something (i.e. illegal hacking is an act of acquiring access and/or information). Hackers, especially those that are motivated by greed and profit, commit a crime that is analogous to trespassing and taking others’ property with the intention of keeping it or selling it. Both of these crimes increase an organization’s security costs and overburden the courts. Secondly, the social stigma associated with shoplifting is not as extreme as for crimes like auto theft, burglary of a residence, and money laundering. And as such we believe that there is a higher probability that our target population has heard discussion of