Chapter 3
The General Theory of Crime and Computer Hacking:
Low Self-Control Hackers?

Adam M. Bossler
Georgia Southern University, USA

George W. Burruss
University of Missouri-St. Louis, USA

ABSTRACT

Though in recent years, a number of studies have been completed on hackers' personality and communication traits by experts in the fields of psychology and criminology, a number of questions regarding this population remain. Does Gottfredson and Hirschi's concept of low self-control predict the unauthorized access of computer systems? Do computer hackers have low levels of self-control, as has been found for other criminals in mainstream society? If low self-control can predict the commission of computer hacking, this finding would seem to support the generality argument of self-control theory and imply that computer hacking and other forms of cybercrime are substantively similar to terrestrial crime. This chapter focuses on the results of a study where we examined whether Gottfredson and Hirschi's general theory of crime is applicable to computer hacking in a college sample.

INTRODUCTION

The evolution of computer technology and the growth of the Internet have both positively and negatively impacted modern life. Although newer technology makes communication and business transactions more efficient, the same technologies have made it easier for criminals, including mal-inclined computer hackers, to victimize individuals and businesses without ever being in the same physical space. Computer hacking, as defined in this chapter, can be viewed as the unauthorized access and use or manipulation of other people's computer systems (Taylor, Tory, Caeti, Loper, Fritsch, & Liederbach, 2006; Yar, 2005a).

Unfortunately, good data do not exist to indicate the frequency and severity of computer hacking (Richardson, 2008), a problem similar to that encountered by white-collar crime scholars

DOI: 10.4018/978-1-61692-805-6.ch003

Copyright © 2011, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

(Benson & Simpson, 2009). Anecdotal evidence, however, illustrates that unauthorized access to computer systems is a serious and growing problem. For example, the 2008 CSI Computer Crime and Security Survey (Richardson, 2008) found that 29% of all security professionals indicated that their systems had experienced unauthorized access in 2007. In addition, the examination of any news website will contain stories covering data breaches, critical infrastructure deficiencies, website defacements, and successful computer hacks. Some of these news stories appear alarmist (see Wall, 2008), but they do indicate that hacking occurs frequently enough to say that it causes substantial damage and that it is not rare. These attacks against computer systems are not only increasing in frequency, but are increasing in sophistication as well (Holt & Kilger, 2008; Schell, Dodge, & Moutsatsos, 2002). To make matters worse, hackers have become more involved with organized crime and state-sponsored terrorism (Holt & Kilger, 2008; Taylor et al., 2006).

Many of the issues and policies regarding cyber security are too technical and beyond the skills and knowledge of traditional criminologists trained in sociology. Criminology's progress in studying cybercrime has been much slower than the evolution of technology itself. One of the greatest benefits that criminologists have made to the cyber security field, however, is the application of criminological theories to different varieties of cybercrime to explore whether traditional criminological theories created for the physical world can help explain crime in the virtual world. If only the medium differentiates crime in the physical and virtual worlds (see Grabosky, 2001), then knowledge previously gained from theoretically-based tests examining terrestrial crime would presumably apply to virtual crime as well; thus, scholars would not have to treat cybercrime as being theoretically different. If terrestrial and virtual crimes were substantially different, traditional criminological theories would not be as useful in the cyber world (Wall, 2005; Yar, 2005b).

In general, research has shown that much of our knowledge regarding crime in the physical world applies to cybercrime as well. For example, research has shown that routine activity theory (Cohen & Felson, 1979) can be applied to both on-line harassment (Holt & Bossler, 2009) and malware victimization (Bossler & Holt, 2009). The general theory of crime (Gottfredson & Hirschi, 1990) and aspects of social learning theory (Akers, 1998) have both been extensively applied to digital and software piracy (e.g., Higgins, 2005, 2006; Higgins, Fell, & Wilson, 2006).

Although the studying of hackers is not new (see Landreth, 1985), there have been few criminological examinations of these groups or their behaviors (Taylor et al., 2006; Yar, 2005a). Most examinations have focused on hackers as a subculture and have largely ignored other theoretical approaches (see Skinner & Fream, 1997, for an exception). Considering that traditional criminological theories have been successfully applied to other forms of cybercrime, our knowledge on computer hacking could potentially be improved if these same theories, such as Gottfredson and Hirschi's (1990) general theory of crime, were examined in relationship to hacking.

Michael Gottfredson and Travis Hirschi's (1990) general theory of crime, or self-control theory, argues that individuals commit crime because they have the inability to resist temptation and, therefore, commit acts having long-term consequences greater than the short-term benefits. Self-control has been demonstrated to be one of the most influential correlates of crime in both the traditional (see Pratt & Cullen, 2000) and digital piracy literature (e.g., Higgins, 2005). Gottfredson and Hirschi would argue that most hacking is simplistic and that hackers take advantage of easy opportunities. Thus, they have characteristics similar to criminals in general. Given this view, the cause of computer hacking is the same as for all other crimes—low self-control.

28 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/general-theory-crime-computer-hacking/46419

Related Content

Spam Image Clustering for Identifying Common Sources of Unsolicited Emails
Chengcui Zhang, Xin Chen, Wei-Bang Chen, Lin Yangand Gary Warner (2009). *International Journal of Digital Crime and Forensics (pp. 1-20).*
www.irma-international.org/article/spam-image-clustering-identifying-common/3906

Spam and Advertisement: Proposing a Model for Charging Intrusion
Dionysios Politis (2009). *Socioeconomic and Legal Implications of Electronic Intrusion (pp. 281-289).*
www.irma-international.org/chapter/spam-advertisement-proposing-model-charging/29370

CBC-Based Synthetic Speech Detection
Jichen Yang, Qianhua He, Yongjian Huand Weiqiang Pan (2019). *International Journal of Digital Crime and Forensics (pp. 63-74).*
www.irma-international.org/article/cbc-based-synthetic-speech-detection/223942

How Much is Too Much? How Marketing Professionals can Avoid Violating Privacy Laws by Understanding the Privacy Principles
Nicholas P. Robinsonand Prescott C. Ensign (2009). *Socioeconomic and Legal Implications of Electronic Intrusion (pp. 108-121).*
www.irma-international.org/chapter/much-too-much-marketing-professionals/29359

AI-Powered Behavioral Analysis in Digital Investigations
(2025). *Exploring the Cybersecurity Landscape Through Cyber Forensics (pp. 189-222).*
www.irma-international.org/chapter/ai-powered-behavioral-analysis-in-digital-investigations/370613