Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2006 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2006

Internet Abuse: A General Theory of Crime Framework

Gregory Schechtman
Washington State University

Kent Marett
Washington State University

John Wells
Washington State University

Internet Abuse: A General Theory of Crime Framework

Gregory M. Schechtman
Washington State University
runnergreg@wsu.edu

Kent Marett
Washington State University
marett@wsu.edu

John D. Wells
Washington State University
wellsjd@wsu.edu

ABSTRACT

Internet abuse is a systemic problem affecting many organizations. Although the definition of Internet abuse can vary across firms, deliberate cyberdeviance against company policy engenders productivity losses and opens firms to increased network surveillance and security costs. As firms become increasingly web-enabled, they become correspondingly more vulnerable to employee cyberdeviance, as more employees are potentially able to abuse their Internet privileges. This paper investigates this under-researched phenomenon and provides a new framework for understanding worker cyberdeviance through the lens of self-control theory in general and Gottfredson and Hirschi's General Crime Theory in particular. Specifically, it proposes that automating the feedback loops of network surveillance systems can decrease Internet abuse by influencing worker perceptions of detection and punishment through faster feedback and improved worker self-control. This study provides an alternative perspective to current research in the area of Internet abuse. Moreover, it provides practical contributions to managers through suggesting methods for organizations to deter such activities.

Keywords

Internet Abuse, Computer Abuse, Self-Control Theory

INTRODUCTION

Cyberdeviance is a drain on organizational resources affecting employee productivity as well as physical assets such as bandwidth and network storage. There are multiple reasons for wanting to understand employee Internet usage and potentially conduct surveillance, the most common of which are (1) loss of productivity, (2) protecting bandwidth, and (3) limiting firm liability. All of these losses can be tied to users accessing inappropriate material on websites, doing personal business on company time, downloading software, and playing video games (Barlow 2003; Gaskin 1998; Urbaczewski 2000). Despite deterrent efforts, during the work day 70 percent of Internet porn is downloaded; 30-40 percent of Internet surfing isn't business related; and more than 60 percent of online purchases occur (Barlow 2003). While both IT adoption (Venkatesh et al. 2003) and Internet addiction are widely studied (DeAngelis 2000; Young 2004), there is scant research examining how to mitigate the negative consequences of Internet abuse.

Underlying this is the question of why users, knowing they are being monitored, persist in their cyberdeviance. To that end, Gottfredson and Hirschi's (1990) General Theory of Crime provides a valuable lens for examining employee Internet abuse. Self-control theory (as it is widely named) is criminology's strongest predictor of crime and analogous behaviors (Pratt et al. 2000). This theory asserts that a person's low self-control leads them to impulsive acts. Prior research has shown people's lack of self-control and need for immediate gratification lead to behavior like drunken driving (Brownfield et al. 1993; Keane et al. 1993), juvenile delinquency (Brownfield et al. 1993), and other adult criminal and imprudent behaviors (Arneklev et al. 1993; Burton et al. 1998; Grasmick et al. 1993; Nagin et al. 1993). Self-control theory's extensive ability to explain crime as well as these analogous behaviors "suggests that Gottfredson and Hirschi's theory is not just a general theory of crime, but of deviant behavior as well" (Jones et al. 2004).

The current research explores Internet abuse. In particular, it investigates situations where users, informed of network monitoring, knowingly choose to abuse organizational Internet policies. This paper theorizes that these actions closely align with deviant criminal motivations. To that end, it adapts self-control theory (Gottfredson et al. 1990) to workplace Internet abuse to provide a new lens for understanding cyberdeviance.

THEORETICAL BACKGROUND

Self Control Theory

In *A General Theory of Crime*, Gottfredson and Hirschi (1990) argue that people who engage in crime are distinguished by their lack of self-control that manifests itself as impulsivity. Self-control is normally the barrier restraining most people from acting on their baser tendencies of wanting to satisfy desires by the fastest and easiest means possible (Gottfredson et al. 1990; Paternoster et al. 1998). Criminals lack this restraint. This is the key tenet behind the self-control theory: criminal acts are quickly accomplished and so appeal to people with self-control issues. Using this lens, low self-control becomes important because it has effects beyond purely criminal acts. Some acts are not criminal, yet still have roots related to impulsivity. Examples include increased accidents, skipped work, gambling, smoking and drinking activities (Gottfredson et al. 1990). The terms "analogous" and "imprudent" behaviors are used interchangeably in the literature (Grasmick et al. 1993) and describe acts that while not criminal still are based upon satisfying immediate desires at the price of long-term goals. Internet abuse is, at its heart, a form of rebellion where users willfully decide to violate company policy. Their illicit act provides immediate gratification. Self-control theory is further applicable to Internet abuse because it also addresses white collar activities such as cyberdeviance (Higgins 2005). According to self-control theory, individuals are rational decision makers weighing the benefits and consequences of behavior (Gottfredson et al. 1990). Cyberdeviance therefore is an individual equation of cost benefit analysis done by people with self-control and impulsivity issues--both explainable through Gottfredson and Hirschi's theory (Higgins 2005).

Deterrence Factors

If impulsive network users make rational choices to abuse their privileges, then the next logical issue becomes how to deter them. Deterrence measures, over and above acceptable use policies, are a useful way to reduce computer abuse (Straub 1990; Straub et al. 1990). However, General Deterrence Theory (GDT), one of the leading theories in criminology explains only a relatively small variance in deviant behaviors (Tittle 1980). As such, researchers (e.g., Peace et al. 2003) have called for more studies that include factors beyond the GDT constructs of perceived certainty and severity of sanctions. The model presented herein fills that gap by integrating GDT and self-control theory. Studies have shown that extralegal sanctions, that is, going beyond organizational policy enforcement, are effective (Bachman et al. 1992; Grasmick et al. 1990). Previous research suggests that illegal behavior decreases as punishment certainty and severity increase (Peace et al. 2003). Certainty is firmly linked to feedback celerity and perceived follow on negative consequences (Nagin et al. 2001). When users fail to see the connection between their acts and punishment, they come to believe punishment will never take place and so are less deterred. This link between cause and effect is vital because punishment certainly more consistently deters crime than punishment severity does. In fact, some researchers believe that certainty of punishment can be as good a deterrent as the punishment itself (Nagin 1998; Williams et al. 1986). If punishment is neither certain nor severe, then it is unlikely that users will conform to network policies (Urbaczewski 2000). Hence, deterrence effectiveness may be seen as a factor of detection certainty, punishment severity, and feedback celerity.

INTEGRATION

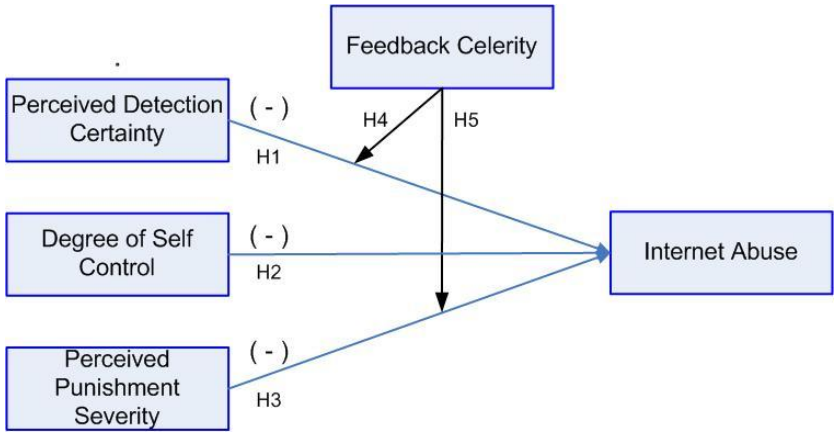

Figure 1. Research Model

Detection Certainty

Research has shown the efficacy of deterrence programs to be related to a person's perceived likelihood of being caught and subsequently punished. For example, research studies specifically looking at illegal software copying have consistently found certain prosecution to deter such criminal behavior (Horney et al. 1992; Paternoster et al. 1985). Yet, deterrence is not limited to certainty of criminal prosecution, but to organizational sanctions as well. Deterring deviant behavior is partly a function of perceived risk of discovery (Holinger and Clark 1983). From this, it is hypothesized that one's tendency to deliberately abuse network access will be related to the likelihood of detection.

H1: High levels of perceived detection certainty will decrease instances of Internet abuse.

Self Control

Past research has shown that individuals with low levels of self-control are more likely to commit acts of deviance. Per self-control theory as described by Gottfredson and Hirschi (1990), such impulsivity is found in individuals who engage in crime and analogous behaviors regardless of the punishment. It logically follows that people with low self-control will be less likely to restrain themselves from deliberate cyberdeviancy. In accord with those concepts, it is anticipated that self-control will be related to the tendency to abuse network access.

H2: Individual self control levels will affect instances of Internet abuse.

Punishment Severity

The impact of punishment severity on deterrence has yielded mixed results (Grasmick and Bursik 1990). Yet, this may be a function of how severity has been modeled rather than the impact of the variable itself. In line with utilitarianism, independent of detection certainty, employees should weigh the personal price they have to pay should their actions be detected. Rational decision makers consider the costs of their actions including severity of the sanctions that accompany it (Blackwell and Grasmick 1994). Based upon this, it is hypothesized that the deterrent effects of any Internet intervention will be based in part on perceptions of how severe the punishment is for detected abuse.

H3: Individual perceptions of punishment severity will affect instances of Internet abuse.

Feedback Celerity

Gottfredson and Hirschi (1990) characterize low self-control as a preference for immediate gratification and as such, future consequences have little influence on current behavior. Moreover, delayed punishments diminish the perceived costs of illicit behavior (Nagin and Pogarsky, 2001). Therefore, the effects of certainty and punishment severity are anticipated to be moderated by the speed with which employees are notified that their abuse has been detected. As Internet abuse takes place over time, workers who receive faster feedback will become increasingly aware that their actions do not go unnoticed. It is anticipated that the faster the feedback, the greater the impact that both perceived detection certainty and punishment severity will have on propensity to abuse.

H4: Feedback celerity will moderate the relationship between detection certainty and instances of Internet abuse.

H5: Feedback celerity will moderate the relationship between perceptions of punishment severity instances of Internet abuse.

METHOD

This study will employ a laboratory experiment varying feedback celerity (near-real time, delayed, no feedback), detection certainty (high, low), and punishment severity (high, low). Students in an undergraduate information system class taught in a computer lab will be given course credit for participating. Before each experiment, subjects will be given a packet of administrative and demographic forms. Grasmick et al.'s (1993) 24-item survey of risk taking behavior, a tested and validated instrument, will be included to measure individual self-control tendencies. While explaining the experiment, the researcher will instruct the students that network monitoring will take place to insure they stay on task and that the computer would be used only for class purposes during the experiment (i.e. not doing email, web surfing, playing games etc). In addition to these activities, Internet abuse will be explained further as going to any web site other than Yahoo or Google search engines or a non ".edu" domain.

In the study, subjects will be required to demonstrate their mastery of the Internet by researching the College of Business entrance requirements for Ivy League universities. The quality of their product will be evaluated and a reward (an Apple IPOD) given for the highest quality work. Punishment severity will be explained by emphasizing that off-topic computer use

will either remove them from contention for the reward (high severity) or cause the instructor to instant message (IM) them to get back on topic (low severity). A confederate will be used in cells manipulating severe punishment and will be verbally notified of the punishment during the session. Commercial automated software will be installed on each workstation that will notify the researcher when students' computer use goes off topic and Windows XP tools will be used to send the "pop-up" IMs. For manipulation checks, during the pilot test debriefing, subjects will be asked to respond with their perceptions of the punishment and detection treatments.

CONCLUSION

The current research is an attempt to understand and combat negative Internet behaviors. It extends current IS understanding of what factors contribute to user propensity for deviant Internet behavior. In doing so, it provides a unique method of deterring Internet abuse. Properly executed, the offered framework may help decrease employee Internet abuse, increase productivity, information assurance, and network security. Finally, this work fills a void in academic research on negative Internet abuse and provides a fundamental starting point for future research that looks, not just at the bright lights, but the shadows they cast as well.

REFERENCES

1. Arneklev, B.J., Grasmick, H.G., Tittle, C.R., and Bursik, R.J. "Low self-control and impudent behavior," *Journal Of Quantitative Criminology* (9:8) 1993, pp 225-247.
2. Bachman, R., Paternoster, R., and Ward, S. "The Rationality Of Sexual Offending - Testing A Deterrence Rational Choice Conception Of Sexual Assault," *Law & Society Review* (26:2) 1992, pp 343-372.
3. Barlow, J., LuAnn Bean, and David D. Hott "Employee "Spy" Software: Should You Use It?," *Journal of Corporate Accounting & Finance*, (14:4), April 15 2003, pp 7-12.
4. Brownfield, D., and Sorenson, A.M. "Self-Control And Juvenile-Delinquency - Theoretical Issues And An Empirical-Assessment Of Selected Elements Of A General-Theory Of Crime," *Deviant Behavior* (14:3), Jul-Sep 1993, pp 243-264.
5. Burton, V.S., Cullen, F.T., Evans, T.D., Alarid, L.F., and Dunaway, R.G. "Gender, self-control, and crime," *Journal Of Research In Crime And Delinquency* (35:2), May 1998, pp 123-147.
6. DeAngelis , T. "Is Internet addiction real? ," in: *Monitor on Psychology*, 2000.
7. Gaskin, J.E. "Internet Acceptable Usage Policies: Writing and Implementation," *Information Systems Management*), Spring 1998, pp 20-25.
8. Gottfredson, M.R., and Hirschi, T. *A General Theory of Crime* MacMillian, New York, N.Y., 1990.
9. Grasmick, H.G., and Bursik, R.J. "Conscience, Significant Others, And Rational Choice - Extending The Deterrence Model," *Law & Society Review* (24:3) 1990, pp 837-861.
10. Grasmick, H.G., Tittle, C.R., Bursik, R.J., and Arneklev, B.J. "Testing The Core Empirical Implications Of Gottfredson And Hirschi General-Theory Of Crime," *Journal Of Research In Crime And Delinquency* (30:1), Feb 1993, pp 5-29.
11. Higgins, G.E. "Can low self-control help with the understanding of the software piracy problem?," *Deviant Behavior* (26:1), Jan-Feb 2005, pp 1-24.
12. Horney, J., and Marshall, I.H. "Risk perceptions among serious offenders: The role of crime and punishment," *Criminology* (30) 1992, pp 5-29.
13. Jones, S., and Quisenberry, N. "The general theory of crime: how general is it?," *Deviant Behavior* (25:5), September-October 2004, pp 401-426.
14. Keane, C., Maxim, P.S., and Teevan, J.J. "Drinking And Driving, Self-Control, And Gender - Testing A General-Theory Of Crime," *Journal Of Research In Crime And Delinquency* (30:1), Feb 1993, pp 30-46.
15. Nagin, D.S. "Criminal deterrence research at the outset of the twenty-first century," in: *Crime And Justice: A Review Of Research, Vol 23*, Univ Chicago Press, Chicago, 1998, pp. 1-42.
16. Nagin, D.S., and Paternoster, R. "Enduring Individual-Differences And Rational Choice Theories Of Crime," *Law & Society Review* (27:3) 1993, pp 467-496.
17. Nagin, D.S., and Pogarsky, G. "Integrating celerity, impulsivity, and extra-legal sanction threats into a model of general deterrence: Theory and evidence," *Criminology* (39:4), Nov 2001, pp 865-891.

18. Paternoster, R., and Brame, R. "The structural similarity of processes generating criminal and analogous behaviors," *Criminology* (36:3) 1998, pp 633-669.
19. Paternoster, R., Saltzman, L.E., Waldo, G.P., and Chircicos, T.G. "Assessment of risk and behavior experience: an exploratory study of change," *Criminology* (23) 1985, pp 417-433.
20. Peace, A.G., Galletta, D.F., and Thong, J.Y.L. "Software piracy in the workplace: A model and empirical test," *Journal Of Management Information Systems* (20:1), Sum 2003, pp 153-177.
21. Pratt, T.C., and Cullen, F.T. "The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis," *Criminology* (38:3), Aug 2000, pp 931-964.
22. Straub, D.W. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3) 1990, pp 255-276.
23. Straub, D.W., and Nance, W.D. "Discovering and Disciplining Computer Abuse in Organizations - a Field-Study," *MISQ Quarterly* (14:1), Mar 1990, pp 45-60.
24. Urbaczewski, A. "An Examination of the Effects of Electronic Monitoring of Employee Internet Usage," in: *Kelly School of Business*, Indiana University, 2000, p. 95.
25. Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. "User acceptance of information technology: Toward a unified view," *MISQ Quarterly* (27:3), Sep 2003, pp 425-478.
26. Williams, K.R., and Hawkins, R. "Perceptual Research On General Deterrence - A Critical-Review," *Law & Society Review* (20:4) 1986, pp 545-572.
27. Young, K.S. "Internet Addiction: A New Clinical Phenomenon and Its Consequences," *American Behavioral Scientist* (48:4), December 2004, pp 402-415.