Cyber-Slacking: Self-Control, Prior Behavior And The Impact Of Deterrence Measures

Joseph C. Ugrin, (Email: jugrin@ksu.edu), Kansas State University
J. Michael Pearson, (Email: jpearson@cba.siu.edu), Southern Illinois University Carbondale
Marcus D. Odom, (Email: modom@cba.siu.edu), Southern Illinois University Carbondale

ABSTRACT

To further our understanding about how to control Internet abuse in the workplace, this study examines how a person's level of self-control leads to cyber-slacking, how deterrence measures commonly used within organizations impact individual decisions to cyber-slack, and how self-control moderates the relative salience of one of the commonly used deterrence mechanisms against cyber-slacking, detection (monitoring) systems. The results suggest that individuals that rate low in self-control overlook potential consequences for abusing the Internet in favor of immediate rewards, thus they have difficulty self-regulating themselves and have a higher propensity to cyber-slack. The results also indicate that detection systems and awareness of the enforcement of sanctions are the biggest deterrents on individual intentions to cyber-slack and detection systems are even more salient to individuals that rate low in self-control.

Keywords: Cyber-slacking, general deterrence theory, Internet acceptable use policy, self-control

INTRODUCTION

The Internet and its associated technologies (hereafter, Internet resources) have, in many respects, altered the way work is performed. They have created a new medium for employees to interact and share information around the globe (Whitty & Carr, 2006). Despite the Internet's ability to impact the communication process and potentially improve the speed and efficiency in which individuals do their jobs, it can have harmful affects on organizations (George, 1996; Griffiths, 2003; Lee & Lee 2002; Lee, Lim & Wong, 2005a). The Internet has introduced new temptations that can dominate an individual's workday (Urbaczewski & Jessup, 2002). The U.S. Treasury Department found that cyber-slacking accounts for nearly 51 percent of employees time on-line (Davis, 2001), and includes activities like answering personal emails, participating in chat rooms, on-line shopping, managing personal finances, or viewing pornography.

Employees appear to have a view of cyber-slacking that seem to be perpetuating its pervasiveness. Surveys of organizations and employees have found that greater than 60 percent of organizations have reprimanded and 30 percent have terminated employees for cyber-slacking (Greenfield & Davis, 2002) yet employees still seem to feel that Internet resources should be available for both work and non-work related activities (Whitty, 2002; 2004). This evidence seems to suggest that rather than reducing costs and increasing a firm's competitive advantage, Internet resources are often abused and may actually cost employers through lost productivity. For this reason, it seems important that we develop a deeper understanding of how individuals feel about Internet use in the workplace, how workplace norms about Internet usage develop, and what mechanisms are available for employers to help reduce the negative impact of the Internet. This paper makes a contribution to the study of business, information systems, and ethics by looking at how an individual's level of self-control relates to his or her propensity to cyber-slack and how self-control and past cyber-slacking behavior impact deterrence mechanisms such as security detection systems.

One could argue that cyber-slacking is a matter of ethics and existing knowledge about ethical decisions may apply. However, new issues typically do not have well developed social norms that drive individual attitudes about them. This may be the case with the Internet and particularly, Internet abuse. Researchers have suggested that existing knowledge about ethical decisions may not hold true for postmodern issues. In many cases, modern issues lack existing norms thus the impact of individual characteristics and situations unique to the decision maker are likely more salient (Dillard and Yuthas, 2002). Dillard and Yuthas (2002 pg. 186) state that "Postmodernism further rejects the deontological concept of reason providing the means by which universally grounded rules, norms, or principles can be ascertained. A decision maker is faced with the ambiguity of ethical choices in the absence of any individual moral responsibility." The advent of the Internet has created a postmodern ethical dilemma; cyber-slacking, that may not have well established norms associated with it to drive individual behavior.

To date, there has been little research on how to reduce cyber-slacking. The research that has been performed seems to show that cyber-slacking is on the rise and efforts to deter it have had limited success. Even when deterrence efforts are successful, they can have other potentially harmful effects (Lee & Lee, 2002; Lee et al., 2005b; Urbaczewski & Jessup, 2002). For example, Urbaczewski and Jessup (2002) found that monitoring activities seem to keep employees from wasting time on non-work related activities but found that this is offset by the negative affect that monitoring activities have on workplace satisfaction and trust. In addition, monitoring activities can have a significant monetary cost (Stewart, 2000).

Acceptable use policies (AUPs) for Internet based applications are a widely used deterrence mechanisms focused on cyber-slacking (Retkwa, 1996). AUPs often consist of guidelines on proper Internet use, usage monitoring, and punishment for inappropriate use (Siau, Nah, & Teng, 2002; Stiefer, 2000). A survey by Greenfield and Davis (2002) found that nearly 87 percent of organizations have AUPs. With such a wide acceptance, we question why is cyber-slacking so pervasive? Various researchers have examined the impact of AUPs and found that in general, AUPs seem to impact Internet usage intentions by making employees aware of what activities are improper and that there are potential ramifications for cyber-slacking (Harrington, 1996; Lee & Lee, 2002; Lee et al. 2005b). In addition, researchers have found that monitoring systems (Harrington, 1996; Lee & Lee, 2002) and the awareness of others being punished for cyber-slacking (Lee & Lee, 2002; Woon & Pee, 2004; Ugrin and Pearson, 2007) have a deterrent effect.

One possible explanation for the pervasiveness of cyber-slacking is that particular deterrence components do not provide enough motivation to slow this activity down. For example, Greenfield and Davis (2002) found that despite the wide use of AUPs, only about half of the organizations they surveyed actively enforce their policies. Thus, one can question how important is enforcement? The same question could be asked about monitoring mechanisms or other deterrence measures.

Another possible explanation for the pervasiveness of cyber-slacking is that deterrence factors don't impact all employees the same. As mentioned, postmodern dilemmas may not have well developed norms and individual factors typically drive behaviors related to those dilemmas, thus it is important to understand how deterrence mechanisms work on different types of individuals. This paper examines the relative impact of deterrence mechanisms on worker's decisions to cyber-slack and how the impact of deterrence mechanisms is altered by the individual's level of self-control and past history (habit) of cyber-slacking. By using a multi-criteria decision methodology (policy capturing), we are able to examine how individuals incorporate different control mechanisms (decision cues) into their decision to cyber-slack and how self-control and habit influence how they apply the cues.

The remainder of this paper is organized as follows. First, we discus cyber-slacking and the factors that influence it. Then, we present a theoretical background on how deterrence mechanisms reduce illicit behaviors such as cyber-slacking. We then examine the impact of self-control and past cyber-slacking behavior on the relative salience of the deterrence factors. Finally, we present our research design, an analysis of results, and conclude by discussing the potential contributions of this research.

CYBER-SLACKING – ANTECEDENTS AND INFLUENCING FACTORS

Cyber-slacking in the workplace has been tagged with various labels including cyber-slouching (Urbaczewski & Jessup, 2002), cyber-loafing (Lim, 2002), junk computing (Guthrie & Gray, 1996), and non-work related computing (Lee et al. 2005). The common thread between these terms is that they all describe unproductive use of the Internet in the workplace. Examples of cyber-slacking are chatting, instant messaging, sending and receiving personal e-mail, online shopping, investment trading, gaming, reading or watching online media, and viewing pornography, among other things.

Research examining the inherent factors that antecede cyber-slacking has yielded a surprising profile of the typical Internet abuser. Stanton (2002) found that men and women are equally likely to abuse the Internet and that Internet abusers are more likely to be highly satisfied employees. In addition, Ugrin, Pearson and Odom (2007) found that executives are more likely to cyber-slack compared to other types of workers. The results of these papers are a far cry from the solitary, discontented, young male that is the typical stereotype of an Internet abuser. In addition, Amiel and Sargent (2004) found that personality types describe the ways in which different types of individuals abuse the Internet. They found that neurotic individuals used the Internet more for information gathering and developing relationships, individuals high in extraversion used the Internet more for tasks related to personal goals, and individuals high in psychoticism used the Internet for more deviant or destructive types of activities. In addition to inherent factors, other factors that have been shown to antecede cyber-slacking include perceived accessibility (Lee et al. 2005b) and affect (Woon and Pee, 2004). Finally, cyber-slacking appears to be a self perpetuating cycle where undetected abuse leads to more slacking in the future. Prior research has found that individuals that have cyber-slacked in the past are more likely to perform it in the future (Lee et al. 2005b; Woon & Pee, 2004).

One factor that has not been looked at in relation to cyber-slacking but has been shown to have a relationship with other types of illicit behavior is self-control. Nagin and Paternoster (1993) introduced self-control as a stable trait that influences one's propensity to commit illicit activities. Nagin and Paternoster's results indicate that individuals that are low in self-control "perceive a higher utility for illicit behavior since the rewards are immediate, and would discount the costs since they are delayed" and "have less developed consciences, making self-censure less effective." They found that self-control has a direct positive impact on individual's intention to partake in several types of illicit behavior, which we expect will be the same when it comes to cyber-slacking. We posit that individuals that are low in self-control will have a greater history of cyber-slacking.

H1: Individuals that rate lower in self-control will have a greater history of cyber-slacking.

Research on deterring cyber-slacking has shown that this behavior can be negatively affected by merely having an AUP (Harrington, 1996; Lee & Lee, 2002; Lee et al. 2005b), installing monitoring mechanisms (Harrington, 1996; Lee & Lee, 2002; Urbaczewski & Jessup, 2002; Whitty, 2004) and enforcement through punishment (Lee & Lee, 2002). Harrington (1996) found that codes of ethics that were specifically related to Internet usage reduced cyber-slacking intentions. Urbaczewski and Jessup (2002) and Whitty (2004) found that monitoring mechanisms that either track or deny access to sites along with monitoring emails reduced cyber-slacking. Lee and Lee (2002) found that individuals that were aware of others receiving punishment for cyber-slacking had a lower propensity to cyber-slack. The next section details the theory behind how deterrence mechanisms like these can reduce cyber-slacking.

DETERRING CYBER-SLACKING: A THEORTICAL PERSPECTIVE

There are two major theoretical perspectives related to deterring illicit behavior such as cyber-slacking, a self-regulated model and an imposed model (Tyler & Blader, 2003; 2005). In short, the self regulated model focuses on an individual's inherent desires to follow the rules. When an individual's values align with the policies set forth by an authority, the individual is more likely to comply (Aalders & Wilthagan, 1997; Gunningham & Rees, 1997; King & Lenox, 2000; Rechtschafen, 1998; Suchman, 1995; Tyler, 2001; Tyler and Darley; 2001; Tyler & Blader, 2003; 2005). The effectiveness of the self-regulated model has received positive evidence in a variety of contexts

(Tyler & Blader, 2003; 2005). However, due to the continued growth of cyber-slacking, it seems that the self-regulated model may not be adequate for this postmodern dilemma. As mentioned, strong social norms related to cyber-slacking may not be well developed and the norms that are developing seem indicate that cyber-slacking is accepted behavior (Whitty, 2002; 2004; Ugrin & Pearson, 2007). In either case, the evidence seems to suggest that deterrence mechanisms need to be imposed by organizations that wish to curb cyber-slacking.

General Deterrence Theory (GDT) provides a theoretical foundation for an imposed model that emphasizes the use of sanctions to deter illicit behavior. GDT is a utility based model that suggests that individuals are rational actors that weigh perceived costs against perceived benefits (Williams & Hawkins, 1986). When employees are presented with opportunities, they select the opportunity that maximizes the total utility of perceived returns versus perceived costs (Tyler & Blader, 2003; 2005; Blair & Stout, 2001). GDT states that deterrence mechanisms that increase the likelihood[1], severity, and celerity of punishment can reduce illicit behavior (Williams & Hawkins, 1986; Beccaria, 1963) (Figure 1). GDT is the theoretical foundation for large body of criminological research that has examined the impact of legal sanctions on illicit behavior and has recently been extended to the impact of sanctions on cyber-slacking (Lee et al., 2005b; Woon & Pee, 2004; Lee & Lee, 2002).

APPLICATION OF GENERAL DETERRENCE THEORY ON CYBER-SLACKING

As mentioned, acceptable use policies (AUPs) are commonly used mechanisms designed to guide employee usage and misusage of Internet resources in the workplace. Stewart (2000) suggested that AUPs should include measures that are strict enough to reduce cyber-slacking but should be tolerant enough to allow employee the potential productivity gains that the Internet can offer. Typical components of an AUP include; (1) an explanation of the scope of the AUP (e.g. who and what does it apply to); (2) a statement defining appropriate use; (3) examples of appropriate versus inappropriate use; (4) a statement defining punishment for inappropriate use; (5) a statement about the extent of monitoring; and (6) a signature of the employee acknowledging that they have received and understand the policy (Siau et al., 2002; Stiefer, 2000).

The extant literature on AUPs is limited, yet other research related to codes of ethics is highly related. In short, researchers have suggested that generic corporate codes of ethics have little impact on employee behaviors yet codes of ethics that are more specific towards a targeted behavior do (Cressy & Moore, 1983; Fimble & Burnstein, 1990; Harrington, 1996). For example, Harrington (1996) found that generic codes of ethics had no impact on deterring computer abuse while IT specific codes of ethics did. Harrington (1996, p. 258) suggests that IT specific codes of ethics "clarify responsibility and so deter unethical behavior."

Case and Young (2002b) examined the impact of signing an AUP. They found that signing an AUP reduces cyber-slacking. In short, they found that 68 percent of survey respondents that worked for organizations that had an AUP were required to sign a statement indicating they were in agreement with the policy and that 53 percent of those individuals indicated that an AUP was an effective deterrent versus only 13 percent of those that were not required to sign a statement related to the AUP.

As mentioned above, an AUP typically outlines the potential sanctions for cyber-slacking. GDT suggests that more severe sanctions will have an increasing degree of deterrence. Thus, when a statement is included in an AUP that outlines severe sanctions that may be handed down for cyber-slacking, individual intentions to cyber-slack are reduced (Lee & Lee, 2002; Williams & Hawkins, 1986; Woon & Pee, 2004). In addition to the mere threat of punishment within a policy, researchers have examined the impact the awareness of enforcement on illicit behavior. Lee and Lee (2002) and Woon and Pee (2004) found that when individuals were aware of others getting punished for cyber-slacking, they had lower intentions to perform similar behavior.

The last deterrence mechanism that is typically used is detection systems that monitor Internet activity. When confronted with choices to commit dishonest behavior, individuals take into account perceived benefits and

1 The general consensus among researchers is that the likelihood of punishment is best operationalized by examining perceived risk of being detected (Hollinger & Clark, 1983)

consequences. However, there must be a strong chance of being caught for consequences to be salient and a set of rules; or in this case an AUP, to be effective (Williams & Hawkins, 1986). Thus, when consequences are perceived to have a greater likelihood, they will have greater deterrence. In general, the consensus about measuring the likelihood of detection is that it is best measured by "exploring the employee's perceived risk of being discovered … not necessarily by investigating the combined threat of apprehension and punishment (Hollinger & Clark, 1983, pg. 402). Urbaczewski and Jessup (2002) studied the impact of monitoring activities and found that they have a significant impact on deterring cyber-slacking.

Although all of these mechanisms impact cyber-slacking, they do not come without costs. For example, monitoring systems have both monetary costs (Stewart, 2000) and costs of reduced employee morale and job satisfaction (Urbaczewski & Jessup, 2002). In addition, not all factors are always implemented. Since deterrence mechanisms come with other consequences, is seems important to not only examine the importance of deterrence mechanisms alone (as shown by the literature cited above) but also how different deterrence mechanisms work relative to one another. Organizations need to understand the relative impact of deterrence mechanisms when making cost benefit decisions on what deterrents they wish to pursue. Based on GDT, it can be conjectured that mechanisms that increase perceptions about the severity and likelihood of punishment will be the most effective. Thus the next step in this study is to develop a hierarchy of the relative impact of the commonly used deterrence mechanisms tested.

THE AFFECT OF SELF-CONTROL AND BEHAVIORAL HISTORY

Individual's self control and prior behavior are not only expected to influence propensity to cyber-slack in the future, they are also expected to change the relative impact of deterrence mechanisms, in particular, the impact of detection systems.

Self-Control

Earlier, we mentioned that Nagin and Paternoster (1993, pg. 472) introduced self-control as a stable trait that influences one's propensity to commit illicit acts. Their results indicate that individuals that are low in self-control "perceive a higher utility for crime since the rewards are immediate, and would discount the costs since they are delayed." We suggest that self-control will also impact the effectiveness of deterrence mechanisms. We expect that deterrence mechanisms that increase the likelihood of detection will have a larger impact compared to other deterrence mechanisms when the respondent has a lower degree of self-control. The rational behind this is that individuals that rate lower in self-control don't view punishment as being imminent; rather they view it as being in the distant future. We suggest that when detection systems are introduced, individuals that rate low in self-control will recognize the potential for punishment that they have previously overlooked. Thus, detection mechanisms will have a greater impact on cyber-slacking relative to other deterrence mechanisms for people that are low in self-control. Beyond this, we have no reason hypothesis any relationships between self-control and other deterrence components *a priori*.

H2: The relative impact of detection systems on individuals that rate lower on self-control will be significantly higher than on individuals that rate higher on self-control

Prior Cyber-Slacking Behavior

As individuals commit abusive behaviors without negative consequences, they begin to form habits that build upon themselves. Habitual abusive behavior leads to further wrongdoing through heightened personal affect (emotion) towards the act which positively influences future activities. Nagin and Paternoster's (1993) results indicated that prior behavior was a strong antecedent to committing theft, drinking and driving, and committing sexual assault. We suggest that habit will also impact the effectiveness of deterrence mechanisms on cyber-slacking. We expect that deterrence mechanisms that increase the likelihood of detection will have a stronger impact compared to other deterrence mechanisms when the respondent has a more active history of cyber-slacking. The rational behind this is that individuals that have previously cyber-slacked without being punished will have

developed a habit for cyber-slacking and, like those that are low in self-control, they will have been conditioned to overlook the likeliness that they will get caught. When a detection system is introduced, it will have an impact on these individuals by bringing the likelihood of punishment to the forefront. Thus, it is posited that that prior behavior will impact the relative salience of detection systems.

H3: The relative impact of detection systems on individuals that have cyber-slacked more often in the past will be significantly higher than on individuals that have cyber-slacked less often in the past.

METHODOLOGY

The relationship between self-control and cyber-slacking and the impact of self-control and prior behavior on the relative salience of detection mechanisms were tested using regression and the relative salience of deterrence mechanisms on reducing cyber-slacking was tested using a policy capturing methodology. Due to the limited use of policy capturing in the information systems discipline, it is discussed in more detail.

Policy Capturing

Policy capturing is a robust method for understanding multi-criteria decisions. In short, policy capturing explains which available items of information are most salient to an individual decision maker. It creates an additive linear model that allows researchers to capture individual decision making policies. It also compares and contrast differences among decision makers and identifies clusters of individuals with similar decision making policies (Karren and Barringer, 2002). The accuracy and acceptance of policy capturing has been evidenced in previous studies in a variety of disciplines. For example, Karren and Barringer (2002) examined 37 policy capturing studies in fields such as organizational behavior, management and psychology, thus illustrating its acceptance as a research tool. Policy capturing has also been used to examine business ethics (e.g. Butler & Cantrell, 1984, Pearson, Crosby, & Shim, 1996) and has been an important method in other business literatures (e.g. Ashton, 1974; Marletta and Kida, 1993) amongst other disciplines.

Karren and Barringer (2002) discuss several advantages to using policy capturing versus other methods (e.g. having individuals rank variables). One key problem with having individuals merely rank variables is the social desirability effect. Policy capturing mitigates the social desirability effect by "indirectly assessing the importance of explanatory variables" (pg. 338). In short, policy capturing regresses a dependent variable on multiple decision cues resulting in a regression equation for each individual and the beta weights of each individual are aggregated resulting in a hierarchy of the decision cues as indicated by their overall average beta weights. Kline and Sulsky (1995, p. 394) state that "the goal of this approach is to understand an individual's decision making "policy" by observing the relationships between the decision cues given to the individual, and the final decision made by the individual and then modeling that relationship using an idiographic multiple regression analysis (i.e., regression analysis carried out for a single individual). The results of the analysis provide a description of how the individual decision-maker weights the various cues to arrive at his or her decision. Thus, within the constraints of the cue information presented, each individual's decision-making "policy" can be observed." The model can be stated as:

$$Y_j = \sum_{i=1}^{n} biXij \text{ where } j=1,2,\ldots\ldots, n$$

The cues (or independent variables), $X_{ij,}$ in this study are (1) existence of an acceptable use policy, (2) the degree of punishment for cyber-slacking, (3) awareness of others receiving punishment for cyber-slacking (4) evidence of detection systems, and (5) a signature by the participant (employee) on the acceptable use policy indicating that they have received it. The final decision (or dependent variable), $Y_{j,}$ is the individual's behavioral intention to cyber-slack.

Procedure

Participants were given 20 unique scenarios covering all combinations of the independent variables (in scenarios where no AUP existed, only the existence of detection systems and awareness of others being punished for cyber-slacking were tested), with differing levels of awareness of the existence of a policy, a statement in the policy stating that employees will be punished for cyber-slacking, awareness of others being punished for cyber-slacking, existence of security and detection systems and the requirement of signing the AUP. The existence of each independent variable, or cue, was indicated by a yes or no statement. Considering each scenario, respondents were asked about whether or not they would use their company's resources for personal use (Appendix 1). Prior history of cyber-slacking and self-control were measured using 7 and 24 item scales respectively. The scales are discussed in more detail in a subsequent section.

Subjects

The sample consisted of 161 total participants made up of 85 individuals from 11 companies that represented diverse industries and organizational sizes along with 76 undergraduate and graduate students at a large mid-western university. Of the employees at the 11 companies, 82 worked full time and 3 worked part time. Five students worked full time and the rest worked part time or were unemployed. Thus we had a diverse sample that represented both full time and part time employees and both young and old.

Following the method outlined in Klein and Sulsky (1995) and Karren and Barringer (2002), an initial test of internal consistency and reliability was conducted on the individual responses by examining the adjusted R square of each individual's responses about how likely they were to cyber-slack. The adjusted R square ranged from 0.121 to 0.987 with an average of 0.590. Responses with an adjusted R square below .50 indicate inconsistent application of the cues and were thus eliminated from further analysis. Based on this, 49 responses were eliminated from the analysis, 18 from students and 31 from employees. Eighteen additional responses were eliminated because the respondents were not employed. The average R square for the remaining respondents was 0.694. Table 1 provides demographics for the initial 161 respondents and those that were retained for further analysis. The respective makeup of the sample on each factor does not appear to change after elimination of the unusable responses indicating that there is no systematic reason for individuals to not respond diligently to the survey.

Table 1. Demographics of Respondents

Gender	(n) = 161	(n) = 94
	(n) Total	(n) Usable
Male	89	49
Female	72	45
Age		
18 – 24	63	31
25 – 29	23	14
30 – 34	12	9
35 – 39	20	12
40 – 44	11	9
45 – 49	10	5
50 or older	22	14
Employment Status		
Full Time	85	45
Part Time	49	49
Unemployed	27	0
Pay Status		
Hourly	52	37
Salary	83	54
N/A	26	3

Measures

Self-control is measured via a 24 question likert type scale (Appendix 2) previously validated by Nagin and Paternoster (1993) and Grasmick et al. (1993). Past cyber-slacking behavior was measured using an 8 item likert type scale with seven questions asking about past history of performing various types of cyber-slacking from chatting and emailing to viewing pornography (Appendix 3). The questions were developed to capture individual's prior behavior on the most common types of cyber-slacking based on the extant literature (e.g. Siau et al., 2002). The scale also included one general question related to the individual's overall degree of cyber-slacking. We computed the Chronbach Alpha for the eight questions resulting in an alpha value of .8028 indicating the scale had adequate reliability.

Hypothesis Tests

To test the impact of self-control on prior history, we performed a regression analysis with self-control as the independent variable and past cyber-slacking history as the dependent variable. We found that overall there was a positive relationship. (R^2 = .317; p < .000). In addition, we found that the relationship holds true for students (R^2 = .358; p < .000) and for workers (R^2 = .180; p = .001). Hypothesis one is supported.

Table 2. Relative Importance of Deterrence Measures

Decision Cues (Deterrence Mechanisms)	Beta Mean	HSD (F = 25.054)*
You are aware of others within the organization being fired for performing non-work related activities on their computer.	-0.37	A
The company employs security detection systems capable of monitoring your computer usage.	-0.35	A
The company's Internet use policy contains a statement stating that you may be fired if you perform non-work related activities on your computer.	-0.26	B
The company employs an Internet use policy that states what types of Internet use is acceptable.	-0.22	B
You are required to sign the Internet use policy indicating that you have read, understand, and will abide by the policy.	-0.12	C

* p < .000 (Items labeled A are significantly different than B and C, B are significantly different than A and C, and C is significantly different than A and B)

To develop the hierarchy of the relative impact of the deterrence mechanisms on individual decisions to cyber-slack, we performed a linear regression for each respondent that supplied a reliable response and averaged the beta weights from the resulting regression equations resulting in an overall hierarchy of the impact of the deterrence mechanisms. The independent variables in each regression were the conditions associated with the five deterrence mechanisms (or cues). The average standardized regression weight, or beta (bi), for each cue indicates its relative importance. Table 2 reports the beta weights of the five deterrence mechanisms on the dependent variable (intention to cyber-slack). Awareness of others getting fired for cyber-slacking had the highest beta weight (-.37), detection systems had the second highest beta weight (-.35), a statement indicating that an individual may be fired for cyber-slacking had the next highest beta weight (-.26), merely having a policy that states what is acceptable had the next beta highest weight (-.22), and finally, signing the policy had the lowest weighting (-.12).

To determine if significant differences existed between the betas, an F-test was conducted. The F-test showed significance (F = 25.05; p < .000), thus differences existed between the betas. Tukey's Honestly Significant Difference (HSD) was calculated to determine which criteria were significantly different from one another. The betas resulted in three groupings (A, B, or C) (Table 2). The betas within the groups were not significantly different from one another but were significantly different from the betas in the other groups. Group A consists of monitoring activities and awareness of others being fired for cyber-slacking. Group B consisted of merely having a policy that

states what are acceptable use and a statement that you may be fired for cyber-slacking. Group C was made up of signing the policy.

To test hypotheses two and three, how self-control and prior cyber-slacking behavior moderate the relative impact of detection systems on an individual's propensity to cyber-slack, we regressed self-control (SC) and prior cyber-slacking behavior (PRIOR) on the beta weights for detection mechanisms (DETECT) controlling for the employees pay status (e.g. if the individual is paid a salary or by the hour) (PAYSTAT), if the individual was full time or part time (FTPT), and if the individual is aware of an AUP at his or her current place of employment (AUP). In short, we control for employment status (full time or part time) and pay status (hourly and salary) because we suspect that they will impact a person's commitment to the organization (Lee and Johnson, 1991; Tsui, Pearce, Porter and Tripoli, 1997) thus impacting their degree of cyber-slacking and likelihood of responding to deterrence efforts. We also suspect that those who are already aware of AUPs at their organizations may be biased by it. Our regression model can be expressed as:

$$DETECT_i = b_0 + b_1 SC_i + b_2 PRIOR_i + b_3 PAYSTAT_i + b_4 FTPT_i + b_5 AUP_i + E_i$$

The results related to the hypotheses two and three show that self-control had a significant effect on the relative impact (beta weight) of security detection systems ($p = .002$), supporting hypothesis two. However, prior behavior had no impact on the salience of security detection systems ($p = .932$), failing to support hypothesis three. Table 3 shows the regression output.

Table 3. Output for Self-Control and Prior Behavior on Detection Betas

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.485(a)	.236	.192	.23131

a Predictors: (Constant), aup, sc, paystat, empstat, prior

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	1.451	5	.290	5.423	.000(a)
	Residual	4.708	88	.054		
	Total	6.159	93			

a Predictors: (Constant), aup, sc, paystat, empstat, prior
b Dependent Variable: detect

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.102	.167		-.613	.542
	Sc	-.008	.003	-.372	-3.181	.002
	Prior	.000	.006	.010	.086	.932
	Empstat	.115	.055	.221	2.097	.039
	Paystat	-.026	.050	-.050	-.522	.603
	Aup	.016	.050	.031	.314	.754

a Dependent Variable: detect

DISCUSSION

This study has shown that self-control has a negative relationship with cyber-slacking and that security detection mechanisms and awareness of enforcement have the largest deterrence on intentions to cyber-slack. The study also shows that greater self-control results in a lower relative impact of security detection mechanisms.

As previously discussed, Individuals that are low in self-control have a lower degree of conscience and have a higher utility for illicit behavior because they place a greater value on the immediate benefits and a lower value on delayed costs as compared to in individual that rates high in self-control. This holds true in the context of cyber-slacking where individuals that rate low in self-control have been shown to have a greater propensity for cyber-slacking. The importance of this for theory is that the impact of the self-control trait holds true with a postmodern dilemma, cyber-slacking. It also supports the notion that postmodern issues are driven by individual factors. The importance for practitioners is that some individuals are more susceptible to cyber-slacking and self-regulation may not be an option for them. However, detection mechanisms are available and with our respondents, enforced sanctions and detection systems had the greatest degree of deterrence (supporting general deterrence theory). Yet unanswered questions remain, such as do the impacts of enforcement efforts and detection systems outweigh their costs monetarily and on employee morale and trust (Urbaczewski and Jessup, 2002; Whitty, 2004).

Finally, the impact of detection efforts is affected by individual levels of self-control. Individuals that rate lower on self-control tend to be impacted more by security detection systems. In general, this means that detection mechanisms have a greater impact on high risk individuals.

In conclusion, detection mechanisms are a strong deterrent against cyber-slacking and they are even more effective on individuals low in self-control who have a higher propensity to cyber-slack. This may add support for the use of detection and monitoring systems; especially in organizations that are already suffering from a great deal of cyber-slacking, despite their potential drawbacks.

This study has some limitations that may be overcome in future research. First, the measure of prior internet activity was based on self-reports reports. Participants may have been not revealed their actual Internet activities, particularly activities related to embarrassing or socially unacceptable behaviors like viewing pornography. Next, the study only examined deterrence mechanisms included in AUPs. Other mechanisms should be explored in the future. Finally, the study treated all types of cyber-slacking equally. For example, answering personal emails was treated the same as viewing pornography. Participant responses may not have been the same over different types of activities. For instance, detection systems may have a strong impact on behavior that may be embarrassing to the participant (such as viewing pornography) and a weak impact on more acceptable types of behavior (such as answering personal emails).

REFERENCES

1. Aalders, M. & Wilthagen, T. (1997). Moving beyond command and control: reflexivity in the regulation of occupational safety and health and the environment. *Law and Policy*, 19, 415-443.
2. Amiel, T. & Sargent, S. L. (2004). Individual differences in Internet usage motives. *Computers in Human Behavior*, 20(6), 711-726.
3. Ashton, R. H. (1974). An experimental study of internal control judgments. *Journal of Accounting Research* (Spring): 143-157.
4. Beccaria, C. (1963). *On Crime and Punishment*. Bobbs Merril: Indianapolis, IN.
5. Blair, M. & Stout, L. (2001). Trust, trustworthiness, and the behavioral foundations of corporate law. *University of Pennsylvania Law Review*, 149, 1735-1810.
6. Butler, J. K. & Cantrell, R. S. (1984). A behavioral model of ethical and unethical decision-making. *Journal of Business Ethics*, 6, 265-280.
7. Case, C.J. & Young, K.S. (2002a). Behavioral factors affecting Internet abuse in the workplace – an empirical investigation. Proceedings of the Third Annual Workshop on HCI Research in MIS, Washington, D.C.

8. Case, C.J. & Young, K.S. (2002b). Employee internet use policy: an examination of perceived effectiveness. Proceedings of the International Association for Computer Information Systems, Fort Lauderdale, FL., October 5, 2002.
9. Cressey, D. R. & Moore, C. A. (1983). Managerial values and corporate codes of ethics. *California Management Review*, 25(4) 66-73.
10. Davis, R.A. (2001). Cyberslacking: Internet abuse in the workplace. Retrieved June 1, 2003 from http://www.internetaddiction.ca/cyberslacking.htm.
11. Dillard J. & Yuthas, K. (2002). Ethics research in AIS. In Accounting as an Information Systems Discipline. In *Researching Accounting as an Information Systems Discipline*, Arnold, V and Sutton, S, ed. American Accounting Association.
12. Fimble, N. & Burnstein, J. S. (1990). Defining the ethical standards of the high-technology industry. *Journal of Business Ethics*, 9, 929-948.
13. George, J.F. (1996). Computer-based monitoring: common perceptions and empirical results. *MIS Quarterly*, 20(9), 459-480.
14. Greenfield, D. N. & R. A. Davis (2002). Lost in cyberspace: the web at work. *CyberPsychology and Behavior*, 5(4), 347-353.
15. Griffiths, M. (2003). Internet abuse in the workplace: issues and concerns for employers and employment counselors. *Journal of Employment Counseling*, 40(2), 87-96.
16. Gunningham, N. & Rees, J. (1997). Industry self-regulation, *Law and Policy*, 19, 363-414.
17. Guthrie, R. & Gray, P. (1996). Junk computing: is it bad for an organization? *Information Systems Management*, 13(1), 23-28.
18. Harrington, S. (1996). The effect of code of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, 20(3), 257-278.
19. Hollinger, R. & Clark, J. (1983) Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Social Forces*, 62(2), 398-418.
20. Karren, R. & Barringer, W. (2002). A Review and Analysis of the Policy-Capturing Methodology in Organizational Research: Guidelines for Research and Practice. *Organizational Research Methods*, 5 (4), 337-361.
21. King, A. & Lenox, M. (2000). Industry self-regulation without sanctions. *Academy of Management Journal*, 36, 502-526.
22. Klien, T & Sulsky, L. (1995). A policy-capturing approach to individual decision-making: a demonstration using professors' judgements of the acceptability of psychology graduate school applicants. *Canadian Journal of Behavioural Science*, 27(4), 393-404.
23. Lee, J. & Y. Lee (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 10(2), 57-63.
24. Lee, O., Lim, K. & Wong, W. (2005a). Managing non-work related computing within an organization: the effects of two disciplinary approaches on employees' commitment to change. Proceedings of the 10th Pacific Asia Conference on Information Systems.
25. Lee, O., Lim, K. & Wong, W. (2005b) Why employees do non-work related computing an exploratory investigation through multiple theoretical perspectives. Proceedings of the 35th Hawaii International Conference on System Sciences
26. Lim, V.K.G. (2002). The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, 23(5), 675-694.
27. Maletta, M. J. & T. Kida. (1993). The effect of risk factors on auditors' configural information processing. *The Accounting Review* (July): 681-691.
28. Nagin, D. S. & Paternoster, R. (1993). Enduring individual differences in rational choice theories of crime. *Law and Society Review*, 27(3), 467-496.
29. Pearson, J. M., Crosby, L. & Shim, J. P. (1996). Modeling the relative importance of ethical behavior criteria: a simulation of information systems professionals' ethical decisions. *Journal of Strategic Information Systems*, 5, 275-291.
30. Rechtschaffen, C. (1998). Deterrence vs. cooperation and the evolving theory of environmental enforcement. *Southern California Law Review*, 71, 1181-1272.
31. Retkwa, R. (1996). Corporate censors, *Internet World*, September, 60-64.

32. Siau, K., Nah, F., & Teng, L. (2002). Acceptable Internet use policy. *Communications of the ACM*, 45, 1, 75-79.
33. Stanton, J. M. (2002). Web addict or happy employee: company profile of the frequent internet user. *Communications of the ACM*, 45(1), 55-59.
34. Stiefer, S.L. (2000). Developing sensible e-mail and internet use policies. *Assessment Journal*, March-April, 53-56.
35. Stewart, F. (2000). Internet acceptable use policies: navigating the management, legal, and technical issues. *Security Management*, July-August, 46-52.
36. Straub, D. & Nance, W. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*, 14(1), 45-62.
37. Suchman, M. (1995). Managing Legitimacy: strategic and institutional approaches. *Academy of Management Review*, 20, 571-610.
38. Tyler, T.R. (2001). Trust and law abidingness: a proactive model of social regulation. *Boston University Law Review*, 81, 361-406.
39. Tyler, T.R. & Blader, S.L. (2003). Can businesses effectively regulate employee conduct?: the antecedents of rule adherence in work settings. Unpublished Manuscript.
40. Tyler, T.R. & Blader, S.L. (2005). Can businesses effectively regulate employee conduct?: the antecedents of rule following in work settings. *Academy of Management Journal*, 48(6), 1143-1158.
41. Tyler, T.R. & Darley, J.M. (1999). Building a law-abiding society: taking public views about morality and the legitimacy of legal authorities into account when formulating substantive law. *Hofstra Law Review*, 28, 707-739.
42. Ugrin, J. & Pearson, J. (2007 forthcoming) Exploring internet abuse in the workplace: How can we maximize deterrence efforts? *Review of Business Journal*.
43. Ugrin, J., Pearson, J., & Odom, M. (2007 forthcoming). Profiling cyber-slackers in the workplace: Demographic, cultural and work related factors. *Journal of Internet Commerce*.
44. Urbaczewski, A. & L. M. Jessup (2002). Does electronic monitoring of employee Internet usage work? *Communications of the ACM*, 45(1) 80-83.
45. Whitty, M. T. (2002). Big brother in Australia: privacy and surveillance of the internet in the Australian workplace. Paper presented at the Internet Research 3.0: Net/Work/Theory. Maastricht, the Netherlands, Oct. 13-16.
46. Whitty, M. T. (2004). Should filtering software be utilized in the workplace? Australian employees' attitudes towards internet usage and surveillance of the internet in the workplace. *Surveillance and Society*, 2(1), 39-54.
47. Whitty M. T. & Carr A. N. (2006). New rules in the workplace: Applying object-relations theory to explain problem Internet and email behaviour in the workplace. *Computers in Human Behavior*, 22, 235-250.
48. Williams, K. R. & Hawkins, R. (1986). Perceptual research on general deterrence: a critical review, *Law and Society Review*, 20(4), 545-572.
49. Woon, I. & Pee, L. (2004). Behavioral factors affecting Internet abuse in the workplace – an empirical investigation. Proceedings of the Third Annual Workshop on HCI Research in MIS.

Appendix 1. Scenario Example

Imagine that you work for a hypothetical company and the following scenario exists in regards to computer deterrence and security measures. Considering the scenario, answer the following question about your personal use of the Internet at work.

Scenario 1 of 20 (Yes means the measure exists. No means the measure does not exist)

-- The company employs an Internet use policy that states what types of Internet use is acceptable.	Yes
-- The companies Internet use policy contains a statement stating that you will be fired if you perform non-work related activities on your computer.	No

-- You are required to sign the Internet Use Policy indicating that you have read, understand, and will abide by the policy.	Yes
-- You are aware of others within the organization being fired for performing non-work related activities on their computer.	Yes
-- The company employs security detection systems capable of monitoring your computer usage.	Yes

1) Based on the scenario, I would use my company's computing resources for personal purposes.

Strongly Disagree		Neutral		Strongly Agree
1	2	3	4	5

Appendix 2. Self Control Scale (Nagin and Paternoster, 1993)

1. I devote time an and effort to preparing for the future.
2. I act on the spur of the moment without stopping to think.
3. I do thinks that bring me pleasure here and now, even at the cost of some distant goal.
4. I base my decisions on what will happen to me in the short run rather than in the long run.
5. I try to avoid projects that I know will be difficult.
6. When things get complicated, I quit or withdraw.
7. I do the things in life which are easiest and bring me the most pleasure.
8. I avoid difficult tasks that stretch my abilities to the limit.
9. I test myself by doing things that are a little risky.
10. I take risks just for the fun of it.
11. I find it exciting to do things for which I might get in trouble.
12. Excitement and adventure are more important to me than security.
13. If I have a choice, I will do something physical rather than something mental.
14. I feel better when I am on the move than when I am sitting and thinking.
15. I'd rather get out and do things than read or contemplate ideas.
16. Compared to other people my age, I have a greater need for physical activity.
17. I look out for myself first, even if it means making things difficult for other people.
18. I'm not very sympathetic to other people when they are having problems.
19. I don't care if the things I do upset people.
20. I will try to get things I want even when I know it's causing problems for other people.
21. I lose my temper easily.
22. When I'm angry at people I feel more like hurting them than talking to them about why I am angry.
23. When I'm really angry, other people better stay away from me.
24. When I have a serious disagreement with someone, it's usually hard for me to talk calmly about it without getting upset.

Appendix 3. Prior NWRC Behavior

1. I have used computers or computer resources for personal use during work time.
2. I have participated in online gaming during company time or using company resources.
3. I have shopped online during work hours or using company computers.
4. I have performed investment trading during work time or using work computers.
5. I have chatted with friends or used instant messaging during work time or using company computers.
6. I have sent or read personal e-mail during work time or using company computers.
7. I have viewed pornography during work time or using company computers.
8. I have read or watched personal online media during work time or using work computers.

NOTES