International Business Research; Vol. 8, No. 3; 2015
ISSN 1913-9004 E-ISSN 1913-9012
Published by Canadian Center of Science and Education

An Experimental Study of Influential Elements on Cyberloafing from General Deterrence Theory Perspective

Case Study: Tehran Subway Organization

Hosseini Mirza Hassan[1], Daraei Mohammad Reza[1] & Mostafa Abdol-Alivandi Farkhad[2]

[1] Department of Management, Payame Noor University, Tehran, Iran

[2] Strategic Management, Payame Noor University, Tehran, Iran

Correspondence: Mostafa Abdol-Alivandi Farkhad, Master in MBA (Strategic Management), Payame Noor University, Tehran, Iran. Tel: 989-122-768-350 or 989-1281-2154. E-mail: mostafa.farkhad@gmail.com

Received: October 25, 2014 Accepted: January 17, 2015 Online Published: February 25, 2015

doi:10.5539/ibr.v8n3p91 URL: http://dx.doi.org/10.5539/ibr.v8n3p91

Abstract

Cyber-loafing is a virtually new phenomenon from the old problem of loafing at work places. The internet has alone made remarkable changes in today's organizations, although has brought many concerns and pitfalls for efficiency and effectiveness in working hours. This study, by the means of General Deterrence Theory and rational choice theory, examined the role of rules and regulations against cyber-slacking and the effect of detection and past enforcement of punishments in Tehran subway organization. The results of this study revealed that severe regulations against cyber-loafers will decrease the intention to cyber-loaf. Moreover, the existence of appropriate detection mechanisms like internet monitoring systems, the awareness of past enforcement of strict retributions among employees, and abusiveness perception of a particular internet activity will substantially lower the chance of being involved in internet abuse in work places.

Keywords: cyber-slacking (-loafing), IUPs, GDT, rational choice theory, theory of interpersonal behavior

1. Introduction

The internet has made irrevocable changes in our life becoming an undeniably vital tool in workplaces by which many work-related activities are automated. Apparently, most clerical duties are strictly dependent upon internet since the cost and duration of them are considerably reduced, and total efficiency of clerks is noticeably improved. However, this phenomenally useful tool is often reported to be abused in most workplaces. Employees' cyber-loafing by participating in non-work related activities such as online shopping, personal investment, social networking, emailing, viewing online media, and viewing pornography. (Blanchard & Henle, 2008; Lim, Teo, & Loo, 2002; Ugrin & Pearson, 2008) In fact, cyber-loafing is employees' use of company-provided Internet access and email for non-work related purposes during working hours. (Lim, 2002) Evidently, professions which involve long hours of working with computers are more likely to be distracted by cyber-slaking. Moreover, in a recent study, employees reported spending at least an hour on nonwork-related activities during a regular working day, and the largest proportion of non-work-related time was spent on the Internet (Salary.com, 2009).

2. Literature

2.1 Acceptable Usage Policy (AUP)

Apparently, the first step to tackle cyber-loafing should be designing an acceptable internet usage policy in organizations. In other words, by the means of approved rules and regulations in terms of internet usage, employees are aware of appropriate and inappropriate online activities and then can make decision if they want to participate or not. Sometimes, human forces are not fully presented with the expected behaviors and surprisingly are asked to display them. Ugrin believes that employees would be more reluctant and apprehensive to participate in any kind of cyber-loafing if they are fully presented with the possible consequences threating the organization (Ugrin et al., 2013). J. C. Ugrin et al. (2013) propose that the threat of potential consequences is likely to be discounted by employees when there is a perception of cultural acceptance of some particular kind of cyber-loafing. (Ugrin et al., 2013) In other words, the compliance between the perceptions of employers and employees plays an important role in deterrence process. Blanchard (2008) claims that if abusive behaviors, as

defined by an AUP, do not match those defined by employees, the AUP and the sanctions within become less effective and require additional measures like detection mechanisms and active enforcement to change attitudes and perceptions. (Blanchard, 2008)

2.2 General Deterrence Model and Cyber-Loafing

GDT (general deterrence theory) is a famous conception in legal system and criminology which proposes the use of punishment as a threat to deter people from offending. Deterrence is often contrasted with retributivism, which holds that punishment is a necessary consequence of a crime and should be calculated based on the gravity of the wrong done. (Azjen, 1985) In other words, this theory places a substantial importance in the role of punishment and legal strict counteraction of unacceptable behaviors, and suggests if the alleviation of illegal or illicit activities is necessary, severe punishments with the minimum amount of leniency is completely vital. GDT has been used in criminal justice, ethics, and most recently, cyber-loafing. (Garret, 2008) General deterrence theory emphasizes the effect of formal sanctions in motivating employees to follow organizational policies. (Han li., 2010) GDT proposes a system in which inappropriate behaviors' punishments are thoroughly defined and by the means of professional detection systems are discovered, and then punished accordingly. The process of determining punishments is certainly involved with the definition of AUPs which must be presented by the officials; each activity which is out of the borders of AUPs is considered to be improper and deserves penalties. In terms of cyber-loafing, GDT is based on an imposed regulatory model, emphasizing regulations that are placed on employees by organizations through the threat of sanctioning. GDT suggests that the threat of sanctions can modify employee actions when potential punishments are weighed against potential benefits of a specific behavior. When confronted with opportunities and related consequences, individuals are believed to be rational actors who weigh the costs versus rewards of taking an action. (Paternoster et al., 1996)

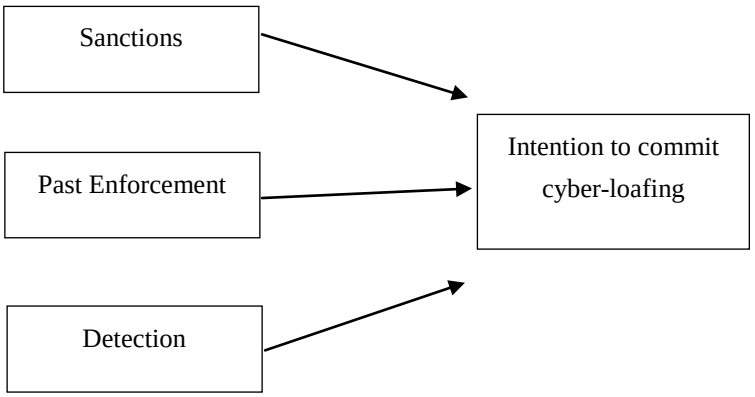

Figure 1. Deterrence model in cyber-loafing

GDT has three components which are proposed to have an influence on illegal behavior; sanctions, detection, and enforcement. (Ugrin et al., 2013).

2.2.1 Sanctions

The primary factor in the GDT model is sanctioning. The certainty of the occurrence of the promised consequences is a determining factor in preventing individuals from being involved in cyber-slaking activities. In other words, the threat of sanctions are effective to the extent they are deemed to be severe. (Garret, 2008) GDT is based on simple economic calculus where more punishment should equal more deterrence. In the context of cyber-loafing, organizations with AUPs that threaten more severe consequences would theoretically see less cyber-loafing. It is proposed that employees will be less likely to cyber-loaf when the potential sanctions for cyber-loafing are perceived to be more severe. (Ugrin et al., 2010).

In fact, this theory considers individuals to be entirely logical with rational thinking who choose an option which has meaningful merits and they consider whether the action has a severe consequence or not; having higher costs, they are more reluctant to involve. In the next section we will more deeply go through the literature of rational choice theory.

2.3 Rational Choice Theory

As mentioned above, general deterrence theory considers all employees as logical thinkers who assess the situation

by identifying if there was a significant merit in doing something. If the outcome of doing a particular action outweighs the costs, it tends to be chosen. The theory then was used in answering some sort of important questions in sociology and criminology. In fact, deviant behaviors were thought to be done in exchange of particular favorable surplus remaining from the differences between the outcome and income of a particular action. This is the main principle of rational choice theory which has been adapted to various contexts to explain deviant behaviors such as income tax evasion, juvenile delinquency, theft, and drunk driving. (Paternoster & Simpson, 1996) Paternoster and Simpson (1996) refined the theory to explain corporate crimes. The theory has two basic premises: "(1) that decisions to offend are based on a balancing of both the costs and benefits of offending and (2) that what are important are the decision maker's perceived or subjective expectations reward and cost" (Paternoster & Simpson, 1996) The first premise suggests that individuals evaluate the expected consequences of multiple alternatives and choose the one with the best outcome. (A. G. Peace, 2003). In other words, individuals are all considered as result oriented persons who logically decide what to do. The second premise emphasizes that deviant behaviors are choices by individuals based on perceived rewards and costs. (A. G. Peace, 2003).

Han li et al. found that there is a compliance between the rational choice made by the offenders, and personal norms and organizational context. (Han li et al., 2010). In other words, Their research model depicts how employees' intention to comply with the Internet use policy is driven by a tradeoff assessment of the risks and benefits of Internet abuses and how the cost–benefit analysis competes with and/or is bounded by the effect of personal moral norms and organizational context factors (A. G. Peace, 2003). The model suggests that employees' IUP compliance intention will increase when 1) employees perceive high threats from formal or informal sanctions or high security risks to their computer or data and 2) employees have high personal norms against Internet abuses. IUP compliance intention may be reduced when employees hold strong benefit beliefs about Internet abuses. The model also suggests that personal norms against internet abuses can be enhanced by the joint effect of organizational norms and organizational identification (A. G. Peace, 2003).

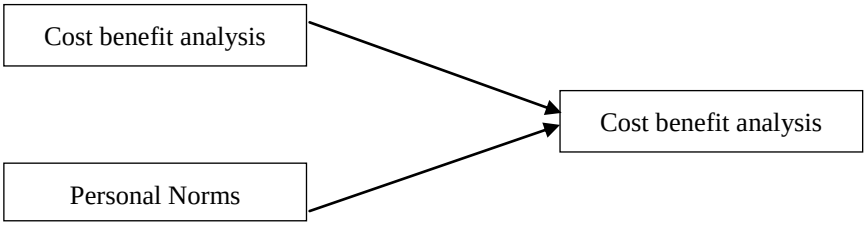

Figure 2. General conceptual model

The result of the mentioned study places importance on the role of training human forces, and enriching their perceptions about ensuing risks of their recklessness. Accordingly, if internet users in an organization become appropriately familiar of the possible perils they pose to the organization, they tend to be reluctant to take the risk of being involved in cyber-slacking. Moreover, and again based on the findings of the research, investments on enhancing and spreading organizational norms and identification would result in employees with higher personal norms who are unlikely to involve in a behavior against IUPs. In other words, various attitudes toward the organization and social norms do, in fact, alter the levels of personal use of the Internet in the organization. (Pee et al., 2008) The results of several surveys showed that consequences, habits, facilitating conditions, and employees' emotions also strongly predict personal use of the Internet at work. (Pee et al., 2008; Cheung et al., 2001).

According to rational choice theory, potential offenders perform a cost–benefit analysis. Benefits act as intrinsic or extrinsic motivation for employees to commit Internet abuse. For example, Websense, Inc. (Websense, 2008) reported high employee traffic to Web shopping sites on the Monday after Thanksgiving holiday as it "saves employees the time and hassle of having to visit a shopping mall, while allowing them to make convenient purchases directly from their desktop." Convenience was perceived to be a significant benefit of non-work-related Internet use (L. G. Pee, 2008). Some employees also visit non-work-related Web sites for entertainment purposes such as downloading music and gaming. These perceived benefits of the Internet abuses may override the effect of sanctions and security threats, and lead to the non-compliance with the Internet use policy (A. G. Peace, 2003).

According to the mentioned information, we developed our first hypothesis saying that:

H1. Intentions to cyber-loaf will be lower when there are strict rules and regulations against cyber-loafing

2.3.1 Detection and Past Enforcement

The study of Ugrin et al. (2013) suggested that the effect of potential sanctions on cyber-loafing will be moderated by an increased likelihood of detection and evidence of past enforcement for less abusive behaviors. (Ugrin, 2013) In other words, employees who realize there are sensitive and professional detection mechanisms are more hesitant to commit a particular kind of cyber-slacking. Moreover, the evidences of past captures and punishments play an important role. In fact, the possibility of being fired decreases the chance of cyber-loafing dramatically. Although sanctions are fundamentally important in making barriers against deviant behaviors, the history of punishments and the severity of them is a determining variable. Han li et al. (2010) says that punishments must be imminent before they have an effect. Consequences that are perceived to be more likely will have greater deterrence. In other words, there must be a strong chance of being caught for a policy to be effective. (William & Hawkins, 1986) In a study that examined the effects of monitoring non-work related computing in general, Urbaczewski and Jessup (2002) found that more monitoring activities resulted in less non-work related computing behavior. (Urbaczewski et al., 2002).

According to the mentioned history of the previous studies above, we developed our second and third hypothesis saying that:

H2. The intention to cyber-loaf will considerably fall when there are records of past enforcement of punishments in an organization.

H3. The intention to cyber-loaf will noticeably decrease when there are advanced internet monitoring systems in an organizations.

H4. The intention to do a particular kind of cyber-loafing will decrease as employees become aware of the high level of abusiveness.

3. Experiment

3.1 Case Study and Participants

The survey was carried out in Tehran subway station. This organization has got near 6000 employees of whom 1200 have got access to the high speed link of the internet. In the survey and based on Cochran formula, 291 participants were chosen. According to the latest observations on the reports of the internet monitoring system already installed, nearly 70% of the clerks in the Tehran subway organization were involved in a particular kind of cyber-loafing.

3.2 Methodology

Cyber-slacking activities in this article were divided into six different activities namely checking personal emails, investment and banking activities, social networks, traditional media, shopping and visiting pornography. At first, we asked participants to rate each internet activities' abusiveness. (By the means of 5 points likert scale from very abusive to not abusive) Afterwards, participants were given a particular scenario and then were asked to rate the chance of each cyber-slacking activities committed by clerks when the given scenario happens. At the end, participants are asked to provide their demographic information.

Participants were faced by the statements below and then by one of the three scenarios:

"Imagine that you work for a company and you are aware of the following information related to computer deterrence and security measures at that company. Consider the three measures presented below and then answer the following questions about how you would use the Internet at that organization." (Answers were formed in the method of Likert scale.)

1) The company's Internet use policy contains a statement stating that you *will be strictly/will not be strictly* punished if you abuse the Internet at work.

2) The company *Employs/Does Not Employ* security detection systems capable of monitoring your Internet activity in the workplace.

3) Others within the organization who have been caught abusing the Internet at work *have been/ haven't been* punished in accordance with the sanction listed above.

4) Imagine that the abusiveness of the each of the cyber-loafing activities is very *High/low* in the organization.

3.3 Variables

Independent variables were strict rules and regulations against cyber-loafing, Detection mechanisms, past enforcement history, and abusiveness of cyber-slacking activities. In fact, the study aimed to examine the effect of

each factor on the possibility of the occurrence of different cyber-slacking activities which are dependent variables.

3.4 Analysis Method

The two main ways of data analysis in this survey were ANOVA (Analysis of variation) and correlation coefficient. The ANOVA is a reliable way of measuring the effect of a particular variable on two or more samples. Here, in this research, we want to examine the effect of two possibilities given in each scenario and decide to find out whether there has been a considerable difference in the time when independent variable happen or not.(In this research Sanctions, Detection mechanism, Past enforcement and Abusiveness) Coefficient correlation also helps us to find out the relationship between dependent and independent variables.

3.5 Reliability and Validity

The questionnaire was adapted from the survey carried out by J. C. Ugrin (2013). In order to examine validity, the questions were also sent to 10 academic persons and after some amendments received their approvals. The reliability was also measured through chronbach alpha in two times; initially, the survey was conducted in a small group of 30 members with the measured alpha of 0.61 which is statistically acceptable. Then, the alpha was measured in the whole survey and 0.67 was calculated as the result.

4. Results

4.1 The Analysis of Abusiveness

There are data about each cyber-loafing activities' abusiveness perception among participants in the survey in the following table. Not surprisingly, watching pornography content was the most disapproved activity, and doing online banking was the least one.

Table 1. The average of the abusiveness of each type of behaviour

No.	Cyberloafing	Abusiveness mean (Percent)
1	Watching pornography	96.8
2	Visiting traditional media and news	61.9
3	Social networks	54.5
4	Personal emails	54.2
5	Online Shopping	47.9
6	Online banking	30.8

4.2 ANOVA Results and Hypothesis Test

We have conducted ANOVA test with SPSS software. The results are as the following tables:

Table 2. ANOVA results of "strict rules and regulations"

Strict rules and regulations							
Dependent variables	Mean (Strict rules)	Mean (Not Strict rules)	Type III sum of Square	DF	Mean Square	F	Sig.
Online Shopping	4.11	4.52	3.125	1	3.125	8.918	0.004
Online banking	3.88	4.63	10.125	1	10.125	25.439	0.000
Personal emails	4.66	4.75	0.125	1	0.125	0.467	0.497
Social networks	4.00	4.63	7.347	1	7.347	15.920	0.000
Watching pornography	1.22	3.13	66.125	1	66.125	91.608	0.000
Visiting traditional media and news	3.77	4.75	17.014	1	17.014	29.068	0.000

Table 3. ANOVA results of "past enforcement history"

Past enforcement history							
Dependent variables	Mean (Strict rules)	Mean (Not Strict rules)	Type III sum of Square	DF	Mean Square	F	Sig.
Online Shopping	3.16	4.08	15.125	1	15.125	38.153	0.000
Online banking	3.05	4.19	23.347	1	23.347	59.369	0.000
Personal emails	4.32	4.44	0.751	1	0.751	0.251	0.321
Social networks	2.94	4.63	51.681	1	51.681	112.368	0.000
Watching pornography	1.00	2.50	40.500	1	40.500	189.000	0.000
Visiting traditional media and news	3.33	4.72	34.722	1	34.722	73.161	0.000

Table 4. ANOVA results of "monitoring systems"

Monitoring							
Dependent variables	Mean (Strict rules)	Mean (Not Strict rules)	Type III sum of Square	DF	Mean Square	F	Sig.
Online Shopping	3.13	4.47	32.000	1	32.000	82.118	0.000
Online banking	3.13	4.36	26.889	1	26.889	70.731	0.000
Personal emails	4.55	4.77	0.889	1	0.889	4.118	0.056
Social networks	2.94	4.58	48.347	1	48.347	72.564	0.000
Watching pornography	1.00	2.58	45.125	1	45.125	127.626	0.000
Visiting traditional media and news	3.55	2.77	26.889	1	26.889	31.841	0.000

Table 5. ANOVA results of "abusiveness"

Abusiveness							
Dependent variables	Mean (Strict rules)	Mean (Not Strict rules)	Type III sum of Square	DF	Mean Square	F	Sig.
Online Shopping	4.22	4.52	1.681	1	1.681	5.550	0.021
Online banking	2.30	4.63	98.000	1	98.000	430.244	0.000
Personal emails	4.36	4.52	0.500	1	0.500	2.026	0.159
Social networks	1.83	4.63	141.681	1	141.681	338.422	0.000
Watching pornography	1.00	3.13	82.347	1	82.347	130.103	0.000
Visiting traditional media and news	2.52	4.75	88.889	1	88.889	395.760	0.000

Table 6. ANOVA results of total independent variables

Sanctions x Past enforcement x Monitoring x Abusiveness					
Dependent variables	Type III sum of Square	DF	Mean Square	F	Sig.
Online Shopping	81.969	7	11.710	32.543	0.000
Online banking	183.833	7	26.262	75.077	0.000
Personal emails	56.653	7	8.093	26.453	0.000
Social networks	291.333	7	51.619	82.957	0.000
Watching pornography	243.635	7	34.805	72.412	0.000
Traditional media and news	183.802	7	26.257	49.334	0.000

Hypothesis one says that Intentions to cyber-loaf will be lower when the potential sanctions for cyberloafing are severe relative to when the potential sanctions are weak. As this is obvious from the data in the table 2, the effect of strict rules and regulations against cyber-loafers is significant in almost all cases apart from checking personal emails. Moreover, the difference between the average possibilities of personal emails in "strict" and "not strict" rules and regulations is not striking (4.66 versus 4.75), which shows that strict rules and regulations are not effective deterrence for this kind of cyber-slacking and participants think that employees would not take any notice of possible outcome in this matter. As a result, this hypothesis is accepted.

To compare with previous study, the result of this survey was somehow different from the survey conducted by J. C. Ugrin et al (2013) as they found significance in all kind of cyber-slacking with the exception of pornography instead of personal emails. However, both studies approved the hypothesis seemingly.

Hypothesis two says that the intention to cyber-loaf will considerably fall when there are records of past punishment records for offenders in an organizations. In table 3, which shows ANOVA results for past enforcement history, personal emails was the only insignificant variables. The averages of personal emails was also too close to each other in the case of the existence and not existence of enforcement history in the organization. (4.32 vs. 4.44) Hence, this hypothesis is approved. Even though, the results of this survey was again different from the survey of J. C. Ugrin et al. (2013) which claimed pornography, personal emails and online shopping were not significant regarding past enforcement history. As a result, their study did not fully support this hypothesis.

Surprisingly, the result of table 4 and 5 regarding Monitoring systems and Abusiveness were exactly the same as the other two tables. They both displayed insignificance in only personal emails (0.056 and 0.156 respectively), and all other variables were completely significant. The averages of personal emails for Monitoring systems were 4.55 versus 4.77, and for Abusiveness were 4.36 versus 4.52. Although, not surprisingly, the result of the study conducted by J. C. Ugrin et al. (2013) was a little different from our result saying that all kinds cyber-slacking were significant for monitoring systems, and the only significant cyber-slacking in terms of abusiveness was online banking (calling Invest in that survey), and all other ones were completely insignificant.

As a result of the information mentioned above, both **hypothesis three** saying that the intention to cyber-loaf will noticeably decrease when there are advanced internet monitoring systems in an organizations, and **hypothesis four** saying that the intention to do a particular kind of cyber-loafing will decrease as employees become aware of the high level of abusiveness, are completely supported. The survey of J. C. Ugrin et al (2013) supported hypothesis three, but completely rejected hypothesis four.

Finally, table 6 showed substantially important data about the combination of all independent variable which were kinds of deterrence mechanisms. In the previous tables, personal emails were the only insignificant cyber-slacking activity which was not affected by any kinds of deterrence mechanisms individually. But surprisingly, in the combination of all independent variables (deterrence elements), personal emails along with all other kind of cyber-slackings showed substantial significance which indicates that even resistant cyber-loafings could be controlled when there is an appropriate combination of deterrence mechanisms.

5. Conclusion

The results of this survey indicate that the compliance of rules and regulations among employees is strongly dependent upon the severity and seriousness of them. In fact, clerks in an organization have a lower desire to cyber-loaf when there are high potential punishments allowed by the rules and regulations. The results also suggest that an advanced and professional monitoring system is highly effective in the reduction of the intention to cyber-loaf. Moreover, past enforcement history is a key to prove the certainty of the legislated retribution. In other words, most clerks estimate the chance of being caught and punished by the records of previous cases. Finally, the awareness of the abusiveness level of a particular kind of cyber-loafing is as effective as the other deterrence factors in this research. As a result, this study suggests that working on building an organizational culture in which some particular online activities are frowned upon could be an effective deterrence.

References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. *Action-Control: From Cognitions to Behavior, 11*, 11-39. http://dx.doi.org/10.1007/978-3-642-69746-3_2

Blanchard, A., & Henle, C. (2008). Correlates of different forms of cyberloafing: Therole of norms and external locus of control. *Computers in Human Behavior, 24*(3), 1067-1084. http://dx.doi.org/10.1016/j.chb.2007.03.008

Garrett, R. K., & Danziger, J. N. (2008a). Disaffection or expected outcomes: Understanding personal internet use during work. *Journal of Computer-Mediated Communication, 13*, 937-958.

http://dx.doi.org/10.1111/j.1083-6101.2008.00425.x

Garrett, R. K., & Danziger, J. N. (2008b). On cyberslacking: Workplace status and personal internet use at work. *Cyber Psychology & Behavior, 11*, 287-292. http://dx.doi.org/10.1089/cpb.2007.0146

Han, L., & Jie, Z. (2010). Rathindra sarathy: Understanding compliance with internet use policy from the perspective of rational. *Decision Support Systems, 48*, 635-645. http://dx.doi.org/10.1016/j.dss.2009.12.005

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing andorganizational justice. *Journal of Organizational Behavior, 23*, 675-694. http://dx.doi.org/10.1002/job.161

Lim, V., Teo, T., & Loo, G. (2002). How do I loaf here: Let me count the ways. *Communications of the ACM, 41*(1), 66-70.

Malachowski, D. (2005). Wasted time at work costing companies billions. Retrieved July 12, 2005, from http://www.salary.com/careers/layoutscripts/crel_display.asp?tab=cre&cat=nocat&ser=Ser374&part=Par555

Paternoster, R., & Simpson, S. (1996). Sanctions threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review, 30*(3), 549-584. http://dx.doi.org/10.2307/3054128

Peace, A. G., Galletta, D., & Thong, J. (2003). Software piracy in the workplace: A model andempirical test. *Journal of Management Information Systems, 20*(1).

Pee, L. G., Woon, I. M. Y., & Kankanhalli, A. (2008). Explaining non-work-related computing inthe workplace: A comparison of alternative models. *Information and Management, 45*, 120-130. http://dx.doi.org/10.1016/j.im.2008.01.004

Ugrin, J., & Michael, P. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior, 29*, 812-820. http://dx.doi.org/10.1016/j.chb.2012.11.005

Ugrin, J., & Odom, M. (2010). Exploring the Sarbanes–Oxley act and intentions to commit financial statement fraud: A general deterrence perspective. *Journal of accounting and Public Policy, 29*(5), 439-458. http://dx.doi.org/10.1016/j.jaccpubpol.2010.06.006

Ugrin, J., & Pearson, J. (2008). Exploring Internet abuse in the workplace: How canwe maximize deterrence efforts. *Review of Business, 28*(2), 29-40.

Urbaczewski, A., & Jessup, L. (2002). Does electronic monitoring of employee internet usage work. *Communications of the ACM, 45*(1), 80-83. http://dx.doi.org/10.1145/502269.502303

Websense. (2004). "Blue Monday" draws high employee traffic to shopping websitesduring work day. Retrieved June 25, 2008, from http://www.websense.com/global/en/PressRoom/PressReleases/PressReleaseDetail/Release=041201792

Websense. (2006). Retrieved March 12, 2009, from http://www.securitymanagement.com/archive/library/websense_technofile0906.pdf

Williams, K., & Hawkins, R. (1986). Perceptual research on general deterrence: Acritical review. *Law and Society Review, 20*(4), 545-572. http://dx.doi.org/10.2307/3053466