Pre-Print Version: Please cite as: Hadlington, L., and Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organisational Information Security? *Cyberpsychology, Behavior, and Social Networking, 20(9)*, 567-571.

Can cyberloafing and Internet addiction affect organisational information security?

Dr Lee Hadlington, De Montfort University, Leicester. United Kingdon

Dr Kathryn Parsons, Defence and Technology Groups, Edinburgh, South Australia.

Key Words: Cybersecurity, Information Security, Internet Addiction, Cyberloafing

Abstract

Researchers have noted potential links between Internet addiction, the use of work computers for non-work purposes and an increased risk of threat to the organisation from breaches in cybersecurity. However, much of this research appears conjectural in nature and lacks clear empirical evidence to support such claims. In order to fill this knowledge gap, a questionnaire-based study explored the link between cyberloafing, Internet addiction, and information security awareness (ISA). A total of 338 participants completed an online questionnaire, which comprised of the Online Cognition Scale (OCS), Cyberloafing scale, and the Human Aspects of Information Security Questionnaire (HAIS-Q). Participants who reported higher Internet addiction and cyberloafing tendencies had lower ISA, and Internet addiction and cyberloafing predicted a significant 45% of the variance in ISA. Serious cyberloafing, such as the propensity to visit adult websites and online gambling, was shown to be the significant predictor for poorer ISA. Implications for organisations and recommendations to reduce or manage inappropriate Internet use are discussed.

1. Introduction

A recent Business Crime Survey highlighted the growing security threat from individuals within the organisation, or 'insider threat'[1]. This finding is presented alongside a realisation by the information security community that the weakest element in the cybersecurity chain is the human end-user[2]. Aligned to this is previous research indicating that improving the information security awareness (ISA) of employees is key to protecting organisations[3]. It is therefore critical to understand the individual factors that may affect ISA. Two concepts, Internet addiction and cyberloafing, are presented in this study as being of critical interest for further research, where cyberloafing refers to non-work related Internet use during work hours and Internet addiction refers to uncontrolled problematic Internet use[4].

1.1 Cyberloafing, Internet Addiction, and Information Security

The concept of cyberloafing has been previously defined as "employees' voluntary non-work related use of company provided email and Internet while working"[6]. Research has linked the potential for cyberloafing activities to aspects of problematic Internet use, in the form of Internet addiction [5,7–9]. Within the workplace, problematic Internet use has been reported to lead to increased mistakes and illogical thought patterns potentially increasing the risk of information security breaches[10]. Despite this potential relationship there is a current lack of research examining the link between cyberloafing, Internet addiction, and ISA.

The prevalence of cyberloafing is widespread, with 44% of employees citing personal Internet use as their top distractor within the workplace[11]. The consequences for such cyberloafing can be varied, with studies often focusing on lost productivity and revenue[6,11]. Indirect costs to cyberloafing have also been noted, including the degradation of system performance due to unnecessary bandwidth use[12], alongside the potential to increase security threats[13,8].

An established a typology for cyberloafing has been previously presented based on its potential impact on the company and its level of legality[6], this being:

- Minor Cyberloafing: included sending and receiving personal email whilst at work, surfing mainstream news websites or financial websites and shopping online.
- Major or Serious Cyberloafing: included the propensity to visit adult websites, maintenance of personal websites, interactions through chat rooms/blogs/personal ads, gambling online, and downloading music.

The findings noted that at least 90% of those employees questioned had received, checked and replied to personal emails during work hours[6]. Less than 10% admitted to visiting chat rooms or adult orientated websites, suggesting that the majority of individuals are engaged in minor cyberloafing activities. However this research is limited due to the self-report nature of the questionnaires, which could mask the full extent of cyberloafing. It could be that individuals are less inclined to admit to engaging in more serious cyberloafing activities due to fear of punitive actions or the need to avoid appearing socially deviant.

Interestingly, research exploring the potential antecedents to cyberloafing has hinted towards a potential role for Internet addiction in its prevalence. For example, it has been noted that both trait procrastination and compulsive Internet use influenced the potential for individuals to engage in cyberloafing[19]. Internet addiction was also noted as being a potential aspect of addictive behaviour viewed as one of the key tenets of the theoretical framework for cyberloafing[8].

As with the work on cyberloafing, research exploring Internet addiction in the workplace has tended to focus directly on the impact for productivity[14]. However additional research has suggested that Internet abuse in the workplace could be a potential extension of employees' activities associated with Internet addiction[15]. Although the relationship between Internet addiction and information security behaviours are yet to be examined, previous research has identified characteristics such as poor impulse control and risk-taking as potential predictors of both behaviours [16–18]

From this previous research a potential confluence could exist between several key aspects of employee behaviour and adherence to information security protocols. Specifically, increased levels of compulsive Internet use may serve to fuel the engagement in cyberloafing activities. In turn, it is these cyberloafing activities that may lead to poorer information security behaviours. These relationships are evaluated in this paper.

1.2 Aims and Objectives

The current research aimed to further examine the link between Internet addiction, cyberloafing and information security behaviours. The research reviewed above indicates a clear potential for technology addiction to 'leak' into work-based activities, and therefore be manifest in aspects of cyberloafing. Consequently, aspects of cyberloafing have also been implicated in the adherence to information security advice as well as having wider security implications on the employee's host organisation. The importance of this work has obvious implications, not only from the perspective of productivity and revenue but also more fundamental information security issues. As the likelihood of engaging in addictive behaviours is linked to individual differences, research of this nature shows how important human factors are in developing and implementing effective cybersecurity practices.

2. Method

2.1 Participants

A total of 351 participants took part in an online survey, with a total of 338 being used in the final sample due to incomplete responses. Participants were recruited through Qualtrics Research Panels (https://www.qualtrics.com/research-core/) and were paid a small honorarium for taking part in the study. The final sample comprised of 165 males and 173 females all employees from the U.K. The age range for participants was 26-65 with a mean of 43.11 years (*SD* = 10.78). All participants reported using a computer as part of their daily work life for at least one and three-quarter hours (approximately 10% of an average 7 hour working day) and were in full or part-time employment. 38% of the participants indicated that they were aware of informal rules to govern the use of digital technology in the workplace, with the remaining 62% stating that there were more formal rules in place.

2.2 Measures

2.2.1. Online Cognition Scale (OCS)

The 36-item OCS is a scale that explores aspects of excessive Internet use[20]. Participants responses are recorded on a 7-point Likert-Scale with 1 = Strongly disagree and 7 = Strongly agree. The OCS has a high level of internal consistency with a Cronbach's alpha of 0.94[3]. In the present study, a Cronbach's alpha of 0.96 was achieved. Possible scores on the OCS vary between 36 and 252.

2.2.2. Human Aspects of Information Security Questionnaire (HAIS-Q)

As a measure of ISA, this study used the HAIS-Q(16,21). All of the questions in this section were responded to on a five-point Likert-type scale, where 1 = Strongly Disagree and 5 = Strongly Agree. Cronbach's alphas of 0.84, 0.84 and 0.92 for Knowledge, Attitude and Behaviour respectively were previously reported[16], with similar scores obtained in the present study ($\alpha_{\text{Knowledge}} = 0.83$; $\alpha_{\text{Attitude}} = 0.92$; $\alpha_{\text{Behaviour}} = 0.90$).

2.2.3. Cyberloafing Questionnaire (CLQ)

This measure contains 22 items exploring the use of work-related computer technology for non-work purposes[6]. Nine items were categorised as minor cyberloafing activities, eight categorised as major[6]. The remaining scale items were retained as fillers but not used in further analyses. Respondents used a 5-point Likert-scale to record the frequency of engaging in cyberloafing during the previous month from 1 = Never to 5 = Frequently. In this study, a Cronbach's alpha of 0.92 was obtained for the Minor Cyberloafing Scale, and 0.95 for the Major Cyberloafing Scale.

2.3 Procedure

The scales outlined above were used to create an online survey with data collection being conducted through Qualtrics Panels between March 6th and March 10th 2017. Participants were invited to take part in the survey and were given a brief introductory statement about the nature of the study. Participants were told that participation was voluntary and they could withdraw at any point during the process. Upon completion of the survey, participants were thanked for their time and given further details of the aims for the study. All incomplete responses to the survey were deleted before the final analysis took place.

2.4 Data Analysis

All statistical analyses were conducted using SPSS (version 22, IBM Corp.).

3. Results

Descriptive statistics for the factors and Pearson's correlations are shown in Table 1, where *n* = 338. There was a significant medium, negative correlation between ISA (i.e., HAIS-Q) and Internet addiction (i.e., OCS) and cyberloafing. This suggests that as ISA increases, Internet addiction and cyberloafing tendencies decrease.

<INSERT TABLE 1 ABOUT HERE>

To determine whether Internet addiction and cyberloafing can predict participants' HAIS-Q scores, a three-stage hierarchical multiple regression was conducted. In line with previous literature linking Internet addiction and potential issues in information security [22,23], OCS was entered at stage one of the regression to control for this variable. Based on previous work, Major Cyberloafing was entered at stage two, and Minor Cyberloafing at stage three[6]. The Durbin-Watson statistic was 2.106, suggesting that independence of errors could be assumed, and values of tolerance and VIF suggested that multicollinearity was not a concern (VIF average = 1.60, tolerance average = .659). Collinearity diagnostics also indicated no multicollinearity.

The results of the regression are displayed in Table 2. In the first stage, with OCS as the only predictor, the model explained 23% of the variance in total HAIS-Q scores. In stage two, introducing Major Cyberloafing explained an additional 22% of the variance. Minor Cyberloafing failed to be a significant predictor for scores on the HAIS-Q. Together, the three variables accounted for 45% of the variance in scores on the HAIS-Q, and both Internet addiction and Major Cyberloafing represented significant negative predictors for scores on the HAIS-Q. As previous research had reported gender differences in cyberloafing tendencies[24], a separate regression was conducted with gender added as a potential predictor for scores on the HAIS-Q. This variable did not add to the model, and is therefore not considered further.

<INSERT TABLE 2 ABOUT HERE>

To examine whether problematic Internet use might also be linked to organisational factors, responses to the following question were examined:

> *"Within your workplace, are you aware of a sets of rules which govern the use of digital technology (such as computers and laptops) and information security (such as sharing passwords or which websites you can view within work time)?"*

127 participants (38%) reported that their organisation has an informal set of rules and 211 participants (62%) reported that their organisation has a formal set of rules. Independent samples t-tests were conducted to compare these groups of participants on problematic Internet use and ISA. As shown in Table 3, participants who stated that their organisation has a formal policy were significantly less likely to exhibit problematic Internet use, both in relation to cyberloafing and Internet addiction. Respondents who reported a formal policy had significantly higher ISA.

<INSERT TABLE 3 ABOUT HERE>

4. Discussion

The results from the present study demonstrate that inappropriate use of the Internet, both in terms of cyberloafing behaviours and Internet addiction, can predict information security. Employees who reported Internet addiction or engaged in cyberloafing had significantly lower information security awareness. The cyberloafing behaviours of interest are considered ‘major’ cyberloafing, and cover behaviours such as visiting adult websites and online gambling. More minor cyberloafing activities, such as sending personal email, were still associated with lower ISA scores, but were not significant predictors in the regression model. Further to this, it was noted that those individuals who had explicit and formal rules governing their use of digital technology in the workplace were less likely to engage in cyberloafing. Finally those individuals who knew about formal rules governing their use of digital technology in their place of employment also scored significantly higher on the scale of information security awareness.

The following sections will discuss the implications of these findings, with a focus on the applied contributions of this research. Finally, the limitations will be presented.

4.1 Internet Addiction in the Workplace

The demonstrated relationship between Internet addiction and poorer engagement in cybersecurity aligns well within the previous literature in the area. However, the majority of this previous research has focused on employee productivity rather than the implications for information security behaviours. Early research noted that those who were categorised as being dependent on the Internet reported severe work-related issues due to spending too much time online[23]. Since this early research, the use of Internet-connected devices and online applications has greatly increased. This is likely to further exacerbate the situation, meaning it is harder for individuals to disengage with the Internet[20,25].

Since the present study indicates that employees’ inappropriate use of the Internet may increase the likelihood of cybersecurity breaches, this highlights the importance of organisations having mechanisms in place to reduce or manage this inappropriate behaviour. The OCS was originally presented as a pre-employment screening mechanism for employers to isolate and potentially exclude those who exhibit addiction to the Internet[20]. However, due to legalities surrounding recruitment, such a process could create an ethical dilemma, especially where the etiology of Internet addiction has been viewed as being akin to substance addictions[26].

In addition, the potential to implement measures to screen out individuals before they are employed fails to mitigate risks that may already be present within the organisation. While some organisations have used employee surveillance, research suggests that these can involve large financial investments and can lower job satisfaction and productivity[9,27]. It has been noted that terminating employees for their Internet abuse could be more costly than the actual misuse[28.] Instead organisations should consider seminars and workshops to help employees identify abuse and seek treatment for addictive behaviours[28].

The vast majority of organisations have clear and explicit guidelines designed to govern employees' use of digital technology within the workplace[25]. However, there is evidence that these policies are poorly understood or enforced by organisations[29]. In the present research, all participants acknowledged rules governing use of digital technology within the workplace, but 38% of respondents indicated these were only informal. Participants demonstrating awareness of a formal set of rules, exhibited higher ISA, and the tendency to engage in cyberloafing was lower. Effective information security education, training and awareness programs can increase employees' ethical integrity and accountability online, and ultimately reduce organisational revenue lost to inappropriate Internet use[28].

4.2 Cyberloafing and Information Security

The findings associated with the impact of cyberloafing on information security present a complicated picture, which warrant further empirical investigation. In the terms of the results from the present study even though minor cyberloafing did not present as a significant predictor for information security, there was still a significant negative correlation between the two. Some aspects of minor cyberloafing have been noted to actually increase aspects of productivity in the workplace[6]. It has been argued that minor cyberloafing can provide a necessary diversion at work, leading to increases in creativity and enhanced learning[30,31]. Even in the instance where individuals may view certain aspects of their personal use of work-based computer services as being socially acceptable, results still demonstrate that they are linked to poorer cybersecurity. A possible explanation for this could be related to an element of risk compensation which has typically been discussed in relation to accident prevention[32]. Mapping the risk compensation hypothesis onto information security, employees may make an erroneous assumption that the systems that the company has put into place give them greater freedom to engage in even more risker activities. This aspect of risk compensation could also be mapped onto organisational culture, where an accepted trade off is made between minor cyberloafing behaviours and lower ISA, in favour of better productivity and job satisfaction levels. Therefore, in weighing the need to complete work tasking with the need to abide by security requirements, organisations might be happy to allow minor cyberloafing[33].

4.3 Limitations

A key limitation with the present research is the use of the term 'Internet addiction' and the measurement of this variable. There are two major approaches to Internet addiction, with the first being the view that it is a growing issue that requires a clinical classification; the second being that excessive or compulsive use of the Internet fuels other aspects of technology addiction, such as online gambling, or gaming[25]. In present work, this argument is accepted as being of critical importance. However in this study, the use of Internet addiction served as a global measure for the individual's potential to engage in activities mediated by the use of the Internet, resulting in negatives outcomes in real life [34,35].

The use of self-report data also presents a possible limitation, particularly where respondents may wish to portray an ideal image of their activities within the workplace rather than the reality. Even though participants were not required to name their employer and were given assurances of anonymity, respondents may still have had an element of reticence to report their actual behaviours. This may be most apparent in the context of cyberloafing activities, and it is assumed that there is still a level of underreporting of this because of the potential negative consequences and implications. In addition, it is important to note that there are also limitations associated with any objective measure of information security behaviours, as incidents are often not detected or reported[36]. Self-report is therefore considered appropriate for this research.

5. Conclusion

The present research examined how Internet addiction and cyberloafing serve to influence attitudes, knowledge and behaviours for information security. The results highlight that Internet abuse and major cyberloafing activities act as key predictors for poor cybersecurity practices that in turn could place the host organisation at risk of a potential breach. As a preventative measure, organisations need to implement effective information security education, training and awareness programs, ensuring that all employees are familiar with the acceptable usage policy for Internet use. While some organisations may implement stringent penalties for serious transgressions, the value of instead providing training to empower employees to recognise Internet abuse and seek treatment for addictive behaviours is discussed as a more cost effective means of reducing or managing inappropriate Internet use.

References

1. BRC. BRC Retail Crime Survey [Internet]. 2015. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Retail+Crime+Survey#0

2. Anwar M, He W, Ash I, Yuan X, Li L, Xu L. Gender difference and employees' cybersecurity behaviors. Comput Human Behav [Internet]. 2016;69:437–43. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0747563216308688

3. Sohrabi Safa NS, Von Solms R, Furnell S. Information security policy compliance model in organizations. Comput Secur [Internet]. Elsevier Ltd; 2016;56:1–13. Available from: http://dx.doi.org/10.1016/j.cose.2015.10.006

4. Keser H, Kavuk M, Numanoglu G. The relationship between Cyber-Loafing and internet addiction. Cypriot J Educ Sci. 2016;11(1):37–42.

5. Ozler DE, Polat G. Cyberloafing phenomenon in organizations: determinants and impacts. Int J Ebus eGovernment Stud [Internet]. 2012;4(2):1–15. Available from: http://www.sobiad.org/eJOURNALS/journal_IJEBEG/arhieves/2012_2/derya_ergun.pdf

6. Blanchard AL, Henle CA. Correlates of different forms of cyberloafing: The role of norms and external locus of control. Comput Human Behav. 2008;24(3):1067–84.

7. Kim SJ, Byrne S. Conceptualizing personal web usage in work contexts: A preliminary framework. Comput Human Behav [Internet]. Elsevier Ltd; 2011;27(6):2271–83. Available from: http://dx.doi.org/10.1016/j.chb.2011.07.006

8. Van Doorn ON. Cyberloafing : A multi-dimensional construct placed in a theoretical framework. Eindhoven University of Technology; 2011.

9. Vitak J, Crouse J, Larose R. Personal Internet use at work: Understanding cyberslacking. Comput Human Behav [Internet]. Elsevier Ltd; 2011;27(5):1751–9. Available from: http://dx.doi.org/10.1016/j.chb.2011.03.002

10. Beard KW. Internet addiction: current status and implications for employees. J Employ Couns [Internet]. 2002;39(1):2–11. Available from: http://doi.wiley.com/10.1002/j.2161-1920.2002.tb00503.x

11. Malachowski D. Wasted Time At Work Costing Companies Billions. Asian Enterp. 2005;14–6.

12. Sipior JC, Ward B. A Strategic Reponses to the Broad Spectrum of Internet Abuse. Inf Manag Strateg Syst Technol. 2002;19(4):71–9.

13. Blanchard AL, Henle CA. Correlates of different forms of cyberloafing: The role of norms and external locus of control. Comput Human Behav. 2008;24(3):1067–84.

14. Griffiths M. Internet abuse and internet addiction in the workplace. J Work Learn [Internet]. 2010;22(7):463–72. Available from: http://www.emeraldinsight.com/doi/abs/10.1108/13665621011071127

15. Stanton J. Company Profile of the Frequent Internet User. Commun ACM. 2002;45(1):55–9.

16. Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T. The human aspects of information security questionnaire (HAIS-Q): two further validation studies.

Comput Secur [Internet]. Elsevier Ltd; 2017;66:40–51. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0167404817300081

17. Egelman S, Peer E. Predicting Privacy and Security Attitudes. Comput Soc Newletter ACM SIGCAS [Internet]. 2015;45(1):22–8. Available from: https://www.icsi.berkeley.edu/icsi/publication_details?n=3738

18. Spada MM. An overview of problematic Internet use. Addict Behav [Internet]. Elsevier Ltd; 2013;39(1):3–6. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0306460313002669%5Cnhttp://www.ncbi.nlm.nih.gov/pubmed/24126206

19. Yan J, Yang J. Trait procrastination and compulsive Internet use as predictors of cyberloafing. 11th Int Conf Serv Syst Serv Manag ICSSSM 2014 - Proceeding. 2014;7–10.

20. Davis RA, Flett GL, Besser A. Validation of a new scale for measuring problematic Internet use: Implications for pre-employment screening. CyberPsychology Behav [Internet]. 2002 [cited 2014 Apr 17];5(4):331–45. Available from: http://online.liebertpub.com/doi/abs/10.1089/109493102760275581

21. McCormac A, Parsons K, Zwaans T, Butavicius M, Pattinson M. Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q). 2016;1–10.

22. Weatherbee TG. Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. Hum Resour Manag Rev [Internet]. Elsevier Inc.; 2010;20(1):35–44. Available from: http://dx.doi.org/10.1016/j.hrmr.2009.03.012

23. Young KS. Internet addiction: The emergence of a new clinical disorder. CyberPsychology Behav. 1998;1(3):237–44.

24. Garrett R, Danziger J. On cyberslacking: workplace status and personal internet use at work. Cyberpsychol Behav. 2008;11(3):287–92.

25. Yellowlees PM, Marks S. Problematic Internet use or Internet addiction? Comput Human Behav [Internet]. 2007 May [cited 2014 Jul 29];23(3):1447–53. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0747563205000439

26. Kuss DJ, Griffiths MD, Karila L, Billieux J. Internet Addiction: A Systematic Review of Epidemiological Research for the Last Decade. Curr Pharm Des [Internet]. 2014;1(4):397–413. Available from: http://www.ncbi.nlm.nih.gov/pubmed/24001297

27. Zoghbi Manrique de Lara P, Tacoronte D V., Ting Ding J-M. Do current anti-cyberloafing disciplinary practices have a replica in research findings?: A study of the effects of coercive strategies on workplace Internet misuse. Internet Res. 2006;16(4):450–67.

28. Young K. Policies and procedures to manage employee Internet abuse. Comput Human Behav. 2010;26(6):1467–71.

29. Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Comput Secur. 2005;24(2):124–33.

30. Lim VKG, Chen DJQ. Cyberloafing at the workplace: gain or drain on work? Behav Inf Technol. 2012;31(4):343–53.

31. Greenfield DN, Davis RA. Lost in cyberspace: the web at work. Cent Internet Stud Psychol Heal Assoc LLC Assist Clin Profr Univ Connect Sch Med Dep Psychiatry. 2002;5(4):347–53.

32. Adams J. Risk. London: UCL Press; 1994.

33. Calic D, Pattinson M, Parsons K, Butavicius M, McCormac A. Naïve and accidental behaviours that compromise information security: What the experts think. In: Furnell SM, Clarke NL, editors. Proceedings of the 10th International Symposium of Human Aspects of Information Security and Assurance. Frankfurt, Germany; 2016.

34. Griffiths MD. Occupational health issues concerning Internet use in the workplace. Work Stress. 2002;16(4):283–6.

35. Lortie CL, Guitton MJ. Internet addiction assessment tools: Dimensional structure and methodological status. Addiction. 2013;108(7):1207–16.

36. Kabay ME. Studies and surveys of computer crime. In: Bosworth S, Kabay ME, editors. Computer Security Handbook. 4th ed. New York: John Wiley and Sons, Inc.;

Table 1: *Descriptive statistics for HAIS-Q, OCS, Minor and Major Cyberloafing*

Construct	*M* (*SD*)	1	2	3	4
1. HAIS-Q	253.22 (36.57)	1	-	-	-
2. OCS	119.55 (43.29)	-.477**	1	-	-
3. Minor Cyberloafing	18.53 (7.58)	-.451**	.436**	1	-
4. Major Cyberloafing	12.34 (7.10)	-.658**	.586**	.672**	1

* p < .05, ** p < .001

Table 2: Summary of hierarchical regression analysis for variables predicting HAIS-Q scores

Variable	β	*t*
Step 1	$F_{(1,\ 336)}$ = 99.13, R^2 = .23**	
OCS	-.48	-9.96**
Step 2	$\Delta F_{(2,\ 335)}$ = 134.70, R^2 = .45**	
OCS	-.14	-2.78*
Major Cyberloafing	-.58	-11.47**
Step 3	$\Delta F_{(3,\ 334)}$ = 89.62, R^2 = .45**	
OCS	-.14	-2.74*
Major Cyberloafing	-.56	-9.21**
Minor Cyberloafing	-.02	-.36

* p < .05, ** p < .001

Table 3: Independent samples t-tests based on knowledge of organisational policy

	Informal *M (SD)*	Formal *M (SD)*	*t*	*p*	*d*
OCS	126.53 (49.04)	115.35 (38.95)	2.19	.03*	.26
Major Cyberloafing	14.41 (8.43)	11.09 (5.82)	4.27	.005*	.48
Minor Cyberloafing	22.81 (9.41)	20.21.(8.31)	2.66	.008**	.32
HAIS-Q	237.98 (37.81)	262.39 (32.60)	-6.05	.001**	-.99

* p < .05, ** p < .001