Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore
An exploratory study

Vivien K.G. Lima,*, Thompson S.H. Teob,1

aDepartment of Management and Organization, NUS Business School, National University of Singapore,
1 Business Link 117592, Singapore
bDepartment of Decision Sciences, NUS Business School, National University of Singapore,
1 Business Link 117592, Singapore

Received 27 May 2004; received in revised form 21 October 2004; accepted 11 December 2004
Available online 21 January 2005

Abstract

The Internet has made a significant impact on work and the personal lives of people around the world. While access to the Internet has changed the ways work can be carried out, it has also increased the opportunities for people to cyberloaf, while under the guise of doing work. Cyberloafing is the act of employees using their companies’ Internet access for personal purposes during work hours. Our study examined the perceived prevalence and seriousness of various cyberloafing activities through a survey of 226 working adults. We examined how employees justify cyberloafing and the organizational regulation of personal Web usage at their workplace. Results suggest that cyberloafing activities that are perceived to be more serious tend to be less prevalent. We also found that the Internet has made the boundary between work and non-work (home) less distinct, facilitating the intrusion of work into home and personal activities into the work domain. Implications of the results are discussed.
© 2005 Elsevier B.V. All rights reserved.

Keywords: Cyberloafing; Internet; Justification; Personal Web usage

1. Introduction

The Internet has been hailed as a technological tool that led to the development of significant opportunities for business and the enhancement of employees’ productivity. Not only has the Internet changed how and where businesses are conducted; it has also altered how and where work is done. While the Internet has brought about many benefits, such as reducing costs, shortening product cycle times, facilitating information access, and marketing services and products more effectively [32,36], its negative effects have also been discussed; they include employees’ concerns about
privacy, loss productivity, and organizational liability resulting from employees’ inbound and outbound Internet activities [19,20,28].

While previous research has examined the social implications of information technology [5], anecdotal evidence has suggested that the advent of the Internet has increased the opportunity for its misuse and that it is thus a double-edged sword that companies should deploy to employees, but with caution. Anandarajan [2] argued that in addition to being an efficient business tool, the Internet provides employees access to the world’s largest playground. While most Internet users feel that activities such as looking up the football scores on the net, or e-mailing a note to a friend, take only a few seconds and should not pose a problem in the bigger scheme of things; often the few seconds can add up to hours and thus becoming a problem to the company. Recent studies revealed that 84% of employees sent non-work related e-mail, while another 90% surfed the Internet for recreational purposes during work hours [37].

These statistics suggest that cyberloafing (using company Internet access for personal purposes during work hours) is prevalent and a pressing issue. Menzel [18] noted that activities such as surfing the Web for entertainment, downloading or viewing obscene materials, and transmitting electronic messages using pen names or pseudonyms are commonly encountered by managers of public organizations in the United States and are considered undesirable and unproductive. Much of management’s concern stems from the idea that cyberloafing depletes employees’ energy and time. A survey of 150 executives in the U.S. showed that the majority reported that employee productivity is impaired because of workplace Internet use for non-work related e-mail, while another 90% surfed the Internet for recreational purposes during work hours [37].

While some attempt has been made to examine the dark side of the Internet, existing studies to date, remain largely unguided by theory and provide little insights as to why this phenomenon occurs. To the extent that employee misuse of the Internet entails considerable cost to organizations and affects employee productivity, it seemed important to find what motivated employees to engage in such behavior so that effective organizational intervention programs and policies could be developed and implemented. In our study, we drew from the theoretical perspectives in the literature on deviant behaviors and neutralization techniques to guide us in understanding employee cyberloafing behavior.

This study is exploratory in nature and has four main objectives. First, we examined the extent to which employees with company Internet access utilized this access for non-work purposes. Second, we examined employee perceptions of the seriousness of different cyberloafing activities. Drawing from research on deviance and delinquency, we reasoned that cyberloafing behaviors that were perceived to be less serious would be more prevalent. Third, we used a theoretical frame to examine how employees justified cyberloafing. In doing so, we also examined the usage of personal Internet access at home for work purposes. Anecdotal evidence and the popular press had suggested that provision of Internet access into the home encouraged the intrusion of work activities there; thus it had made the boundary between work and non-work less distinct. For example, a recent survey conducted at the University of Maryland [21] suggested that while American employees do use the Internet at work for personal business, they also spent more time at home on work-related tasks. These results are instructive in that they suggested that the Internet has been shifting work to home more than personal activities to work. We believe that this is a commonly cited argument of employees when rationalizing cyberloafing behavior.

Our research examined the extent of workplace Internet usage regulation in Singapore. Extant studies in workplace deviance literature suggest that organizational control mechanisms, policies, and procedures play an important role in regulating employees’ behaviors. Thus, it seemed interesting to examine the extent to which organizations regulated employee Internet usage at work and employee responses to any such regulation.

2. Theoretical background

Previous research has investigated the motivation for Internet usage [35], factors affecting Internet usage
as well as the effects of age on Internet usage [33].

Cyberloafing (both surfing the Web and checking e-mail for personal use at the office) constitutes an unproductive use of time and therefore can be considered a deviant workplace behavior. Workplace deviance refers to voluntary acts undertaken by organizational members that violate significant organizational norms, adversely affecting the well-being of organizations and/or their members. We categorize cyberloafing under the rubric of production deviance, which includes relatively minor, organizationally harmful misbehavior, in the typology developed by Robinson and Bennett [24]. The other three are (a) property deviance, unauthorized taking or damage of tangible company property; (b) political deviance, employees’ engagement in social interaction that puts other individuals at a personal or political disadvantage; and (c) personal aggression, aggressive or hostile behaviors towards others.

Production deviance is a perennial and costly phenomenon that has long existed in organizations; e.g., Snyder et al. [30] found this when employees admitted to malingering on the job. In fact, the ABA Banking Journal [1] gave a comprehensive list of types of loafers at work, including telephone chatters, restroom-minded people, and long lunchers.

With the availability of the Internet, however, production deviance has taken on a new form. Employees can now maintain the guise of being hard at work while surfing Websites for personal interests and purposes. Cyberloafers need not be absent from the office, as long lunchers are. They also need not worry about the visibility of their loafing, as have those who stand by the water cooler to chat. They may, however, inadvertently spend much time surfing the Internet, moving from one Website to another, etc. They might even expose the organization to legal liabilities and to the dangers of a computer virus, etc. These factors suggest that cyberloafers may pose a greater “threat” to organizations than other types of loafers.

The theoretical perspective of the literature on deviance explained that individuals often engaged in such behaviors if it were perceived to be less serious in terms of its consequences [8]. Hollinger and Clark [12] found that employees were more likely to engage in less serious forms of theft (i.e., of inexpensive items). In a similar vein, Lim and See [17] found that academic cheating was perceived by students to be less serious than plagiarizing or not contributing equally in a group project. The theoretical explanation is that people do not hesitate to engage in acts if they perceived that the consequences to the organization are minimal and entail little cost.

Research on deviance and neutralization techniques has shown that individuals invoke neutralization techniques to assuage their guilt when engaging in acts of deviance. These techniques are rationalizations that individuals invoke in order to convince themselves and others that their deviant behaviors are justifiable and/or excusable [10]. They wish to project a positive image and protect themselves from self-blame and guilt [25]. In this way, neutralization makes it easier for people to engage in deviant acts.

Sociologists, Sykes and Matza [29] explained that engaging in such rationalizations will allow individuals to “deflect”, “neutralize”, or “turn back” censure stemming from their actions. Through this process, individuals are able to engage in antisocial behavior while retaining their self-image. We argue that approaching the issue of cyberloafing from the theoretical perspectives offered by deviant behavior and neutralization techniques therefore helps to further understand why cyberloafing among employees continues to prevail despite the presence of extensive organizational rules and procedures designed and implemented precisely to keep such behavior to a minimum. We, therefore, reasoned that employees rationalized away their cyberloafing activities by invoking neutralization techniques to assuage any guilt.

3. Context and scope of study

Singapore provides an ideal context for our study because of the decision of its government to fully wire the country. With widespread Internet access both at work and home, Singaporeans are generally Internet-savvy, making them a suitable group to examine.

Based on existing literature, we expected cyberloafing to have four key aspects: prevalence, seriousness, justification, and regulation as illustrated in Fig. 1. Our framework, thus, consisted of three concentric circles. At its core is cyberloafing in the
organization. In the second layer there are three key aspects of cyberloafing: prevalence, perceived seriousness, and justification. An understanding of these three aspects is crucial in formulating appropriate organizational regulations to deal with it (as shown in the outermost layer).

In this framework, we predicted that cyberloafing behaviors perceived to be more serious by individual employees would be less prevalent. We also predicted that employees would have different ways to justify it (classified under various neutralization strategies) and that clear Internet usage policies were needed to regulate cyberloafing in the workplace.

4. Method

4.1. Sample and procedures

Data were collected from working adults with access at work to the Internet. This method of data collection was deemed appropriate for two reasons:

1. It provides access to an enormous pool of employed adults who are Internet-savvy and able to cyberloaf if they are inclined to do so.
2. Previous research has shown that people exhibit lower social desirability when they respond to an online rather than a paper-based questionnaire [14]. Therefore, as we are trying to elicit responses to behaviors, which may reflect negatively on respondents, we decided to use an electronic questionnaire to ensure that social desirability was kept to a minimum and anonymity ensured.

Prior to posting the questionnaire on the Internet, the instrument was first pre-tested with two undergraduate Internet users. While no major problem was detected, several minor modifications were made regarding the clarity of some items as well as the overall presentation of the survey. The second round of pre-test was conducted using three working adults. No major adverse comments were raised by them; thus the survey instrument was deemed ready for actual respondents.

Data were obtained through a combination of an Internet-posted survey and focus group interviews. The survey site was publicized in various newsgroups. Hyperlinks were also placed on the ‘What’s New’ page of Singnet (an Internet Service Provider in Singapore) as this was one of the more popular sites for local Web surfers.

About 3 months after the survey was first posted, focus group interviews were conducted with 30 working adults (six groups of five respondents each). These working adults were selected randomly from respondents who agreed to be interviewed. The purpose of the interviews was to elicit comments to enhance our understanding of cyberloafing in the workplace. Each interview session lasted an average of 1 h and was structured to focus on issues that involved the use of the company’s Internet facilities. Respondents were asked what they thought about the use of the company’s Internet for personal purposes, whether policies about use of the company’s Internet facilities existed, and to indicate reasons or occasions in which it would be correct for employees to use the company’s Internet for non-work reasons.

Respondents were 226 working adults who had access to the Internet at work. The average age of respondents was 28 years (S.D. = 6). About 80% of respondents had at least a diploma or a bachelor’s degree; 52% were males. Approximately 40% worked for organizations in the public sector, while the rest worked in the private sector. Fifty-five percent worked in the IT industries, 25% were from the service industry, while finance and manufacturing comprised the rest.

Respondents reported that, on average, they used the Internet for about 2.7 h each day while at work; they had been using the Internet for about 3.1 years. All respondents reported that they also had access at home.
Our sample was comparable to studies conducted on Internet users both locally and in the U.S.; people were of about the same age and educational level. For example, the majority of respondents in Teo et al.’s [34] study were in the 16–30 years age group, while the respondents in the Graphics, Visualization & Usability Centre [9] study averaged about 38 years of age. Additionally, both studies found that the general Internet user was college (or equivalent) educated.

4.2. Instrument

We captured the following data in our survey in the questionnaire that was built by developing and adapting scales from previous research [15,17]:

1. prevalence of cyberloafing;
2. perceived seriousness of cyberloafing;
3. justification for cyberloafing; and
4. regulation of cyberloafing.

The prevalence was measured on a 6-point Likert scale ranging from (0) never to (5) constantly; while perceived seriousness was measured on a 6-point scale ranging from (0) not serious at all to (5) most serious. The justification was assessed by asking respondents whether it is acceptable to cyberloaf and its duration. Respondents were also asked to list why and when they felt that cyberloafing was permissible. Their responses were then coded by the two researchers and supplemented with material from the focus group interviews. On items pertaining to regulation, respondents were asked to report whether their organizations have policies regulating cyberloafing, and whether they knew of anyone, professionally or personally, who had been disciplined for cyberloafing. Also, we asked respondents to indicate whether it was possible to regulate Internet usage at the workplace and whether these regulations were acceptable.

5. Results

5.1. Prevalence of cyberloafing

Respondents were asked to report on their perceived prevalence of a list of activities at their workplace. These were grouped into two main categories:

(i) browsing, which included using company Internet access to browse non-work related Websites while at work; and
(ii) e-mailing, which included sending, receiving and checking non-work related e-mails while at work.

We performed confirmatory factor analysis (CFA) to ascertain the underlying factor structure for the cyberloafing items. Two factors, accounting for 62% of the variance, were retained. We also assessed reliability using Cronbach alpha. The results are shown in Table 1.

The first factor, browsing activities, consisted of 10 items (α = 0.85) pertaining to how often individuals used the Internet during working hours to surf various non-job related Websites, such as those which are investment-, sports-, or entertainment-related.

The second factor, e-mailing activities, include three items (α = 0.90) which assess how often they sent and checked personal e-mails during working hours. Results of CFA suggested that there are indeed two factors underlying the construct, providing evidence of construct validity. The Cronbach alpha value was above 0.70, indicating that reliability is adequate [22].

Turning now to the descriptive statistics, Figs. 2 and 3 summarize the mean for prevalence of cyberloafing.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Factor analysis and reliability assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsing activities (eigenvalue = 5.2, variance explained = 47.7%, α = 0.85)</td>
<td>Browsing activities (eigenvalue = 5.2, variance explained = 47.7%, α = 0.85)</td>
</tr>
<tr>
<td>Sports related Websites</td>
<td>0.89</td>
</tr>
<tr>
<td>General news Websites</td>
<td>0.85</td>
</tr>
<tr>
<td>Entertainment related Websites</td>
<td>0.83</td>
</tr>
<tr>
<td>Download non-work related information</td>
<td>0.75</td>
</tr>
<tr>
<td>Non-job related Websites</td>
<td>0.74</td>
</tr>
<tr>
<td>Shop online</td>
<td>0.70</td>
</tr>
<tr>
<td>Look for employment</td>
<td>0.65</td>
</tr>
<tr>
<td>Adult-oriented (sexually explicit) Websites</td>
<td>0.60</td>
</tr>
<tr>
<td>E-mailing activities (eigenvalue = 1.5, variance explained = 14.3%, α = 0.90)</td>
<td>E-mailing activities (eigenvalue = 1.5, variance explained = 14.3%, α = 0.90)</td>
</tr>
<tr>
<td>Check non-work related e-mail</td>
<td>0.90</td>
</tr>
<tr>
<td>Send non-work related e-mail</td>
<td>0.87</td>
</tr>
<tr>
<td>Receive non-work related e-mail</td>
<td>0.87</td>
</tr>
</tbody>
</table>
Findings suggest that using company Internet access to browse non-work related Websites (mean = 3.42), general news Websites (mean = 3.33), entertainment Websites (mean = 2.92) and sports Websites (mean = 2.35) were perceived to be among the most prevalent. The least common cyberloafing activities include using the company Internet to browse adult-oriented Websites and shopping for goods. This may be due to restricted access by proxy servers, put in place by the organization. Organizations may also have mechanisms to track visits to such Websites, sending a strong message to employees that such activity will not be tolerated. However, since the data did not allow us to test for such mechanisms, this explanation is merely speculative.

The low mean prevalence for shopping online (mean = 1.30) suggests that it is a low level activity among respondents. Previous studies suggest that...
inherent risks (lack of security) associated with online shopping, need to touch and feel products before purchase, and shopping as a social activity [23,31] inhibit online shopping. However, this explanation must remain, at best, in the realm of speculation.

Turning now to e-mailing activities, receiving non-work related e-mails (mean = 3.11) had the highest mean prevalence, followed by checking personal e-mails (mean = 2.93) and sending non-work related e-mails (mean = 2.09). Respondents explained that they could control what and when to send, but it was difficult to control what others sent.

5.2. Perceived seriousness of cyberloafing

Not all cyberloafing activities were perceived to be equally serious. Specifically, only 5 of the 15 behaviors surveyed had means above the midpoint (2.5), suggesting that only these five were considered serious.

Findings suggested that respondents perceived using company Internet access to browse adult-oriented Websites (mean = 3.89) and playing online games (mean = 3.01) were quite serious. Shopping for personal goods and engaging in online chat and games were also perceived to be more serious than activities such as surfing general news sites, sports, and entertainment sites.

E-mailing activities such as sending personal e-mails (mean = 1.89), checking personal e-mails (mean = 1.65), and receiving personal e-mails (mean = 1.52) were rated less serious.

In general, there appears to be an inverse relationship between the prevalence of an activity and the seriousness of engaging in it. Results of correlational analyses presented in Table 2 support this relationship: activities that are not permitted by the company (hence more serious) tend to be less prevalent.

5.3. Justification of cyberloafing

We also asked respondents to state when and why it was acceptable to engage in cyberloafing at work. Their responses can be grouped according to the following techniques of neutralization proposed in past literature.

| Table 2 Correlation between prevalence and perceived seriousness of cyberloafing items |
|-----------------------------------------------|--------------|
| Cyberloafing items                          | Correlation  |
| **Browsing**                                 |              |
| 1. Visit non-job related Websites            | -0.25*       |
| 2. Visit general news Websites               | -0.28*       |
| 3. Visit entertainment-related Websites      | -0.20*       |
| 4. Visit sports-related Websites             | -0.19*       |
| 5. Instant messaging/chat online (IRC)       | -0.32*       |
| 6. Download non-work related information     | -0.10        |
| 7. Look for employment                       | -0.18*       |
| 8. Shop online                               | -0.21*       |
| 9. Play online games                         | -0.21*       |
| 10. Visit adult-oriented (sexually explicit) Websites | -0.36*       |
| **E-mail**                                   |              |
| 1. Receive non-work related e-mail           | -0.18*       |
| 2. Check non-work related e-mail             | -0.19*       |
| 3. Send non-work related e-mail              | -0.10        |

* p < 0.05.

5.3.1. Normalization (i.e., everyone else is doing it)

About 88% of respondents reported that it is acceptable to use company Internet access to cyberloaf when they perceived that everyone else engaged in it. Such reasoning is termed normalization and appeals to an assertion of generality and commonly practiced behavior.

Comments obtained from focus group interviews supported this:

- “Almost everyone in my company engages in some form of cyberloafing or other; I don’t see anything wrong in it.”
- “I would say that 99.9% of people in my organization use company Internet access for their personal use. It becomes the norm rather than exception.”
- “E-mail has become an essential part of our lives. So it is normal for everyone to use e-mail for work and non-work related activities during office hours.”

The idea underlying this is consistent with social theories. Indeed, social information processing theory suggests that employees’ behaviors are, to a large extent, guided by values, norms, and expectations prevalent in the work environment [27]. In a related manner, social learning theory suggests that indivi-
duals learn to behave by observing others’ behaviors and their consequences [4]. Thus, employees who received cues from their work environment that certain levels and types of cyberloafing activities are prevalent and permissible are more likely to “normalize” such behaviors, making it easier to engage in them.

5.3.2. Minimization (i.e., it is only for a few minutes and does not hurt anyone)

Other excuses provided by respondents can be categorized under minimization. Some comments obtained from respondents included:

- “It’s only for a few minutes; I don’t see how it (cyberloafing) can hurt anyone.”
- “I don’t see how cyberloafing can hurt the company. I do not engage in it for long periods of time. It is not as if I do it for a few hours.”
- “Doing it (cyberloafing) once in a while is OK.”
- “My company has broadband Internet access. So accessing the Internet is very fast. So not much time is wasted.”

Such employees generally trivialize and downplay the consequences of their behavior on the organization. A majority stated that it was acceptable to “cyberloaf a little during the working day.” An average of about 32 min per day was deemed to be acceptable. Most respondents justified their activities on the grounds that they only intended to engage in the activities for a short time, and viewed it as a respite from work. Indeed, research on antisocial behaviors in the workplace has suggested that the minimization technique is one of the most commonly invoked justification to excuse errant behavior [11]. This is an interesting finding as it suggests the relative ease with which our respondents excused their behavior.

5.3.3. Superordination (i.e., tit for tat)

A third excuse pertained to superordination (that the employees had been unfairly treated). Previous research found that employees become disgruntled when they thought that the effort expended on their jobs exceeded the rewards received. Hence, they were motivated to restore this perceived inequity [3]. Indeed, 89% of our respondents reported that it was acceptable to cyberloaf if they had been unjustly treated, and another 95% reported that it was acceptable if they are underpaid. Results of this study are consistent with those by Lim et al. [16]:

- “I am currently underpaid for the number of hours I need to work. Hence, the company should not mind if I use the Internet for non-work related purpose while in office as I hardly have personal time at home.”
- “My boss expects me to put in overtime work practically everyday. So it should be OK to cyberloaf once in a while to relieve stress from too much work.”
- “Instead of hiring new staff to replace those who have resigned, the work is distributed among existing staff. Yet, our salary was not increased. So using the Internet for non-work related activities should not be a big deal.”

5.3.4. Shifting work home

Respondents with Internet access at home (including those with access at work) spent an average of 4.5 h per week at home on work-related activities. Findings suggest that these working adults spend an average of 3.2 h per week using company Internet access on personal activities, while they were supposed to be working. Our findings are consistent with results of NTRS which found that on the average, American working adults with both home and work Internet access spent an average of 5.9 h per week at home on work activities and 3.7 h per week on personal activities at work. Such findings are instructive; they suggest the permeability of the boundary between work and home. Management should be mindful that employees are increasingly spending their time outside work using their home Internet to engage in work activities: although they do not telecommute, they are increasingly bringing work home. Indeed, respondents stated:

- “I think I spent more time at home doing work than running personal errands while I am supposed to be working.”
- “Whatever time I used at work to cyberloaf, I more than compensate for it by working at home.”
- “I am online practically everyday during and after office hours. Hence, it is common for me to mix work and non-work both in the office and at home.”
Apparently, the availability of the Internet has led to the workplace and home becoming increasingly enmeshed.

5.4. Regulation of cyberloafing

Turning now to the issue of regulation, the majority of respondents (82%) reported that they did not know anyone, professionally or personally, who had been disciplined due to non-work related Internet usage at the workplace. Findings suggest that organizations do discipline employees however, since approximately 18% of respondents were aware of colleagues warned about cyberloafing.

When asked about regulating Internet usage at the workplace, respondents appeared to be divided: while 58% believed that this was possible, 42% reported otherwise. They explained that they would perceive a lack of trust if companies monitored their Internet activities, and viewed Internet regulation with resentment.

Approximately 45% of respondents reported that their organizations had policies on Internet usage, while 40% indicated otherwise. Compared to findings in the U.S., where 87% of companies surveyed indicated that they had formal Internet usage policies [13], this figure is relatively low. Interestingly, 15% of respondents indicated they were unaware of the existence of any policies governing Internet usage at their workplace. This suggests that, while policies may exist, they are not adequately and effectively communicated to the employees. This not only defeats the purpose of having policies, but also makes it difficult to enforce them when necessary.

Finally, our results suggested that among respondents whose organizations had policies to regulate Internet usage, 64% reported that they found this policy acceptable, 23% reported they were unsure, and 13% did not find it acceptable.

6. Contributions

Our study contributed in several ways. First, we extended previous research by examining the perceived seriousness of cyberloafing (in addition to its prevalence). Results suggested that respondents perceived some forms to be more prevalent than others; and that not all activities were equal in terms of there perceived seriousness. By examining both the prevalence and perceived seriousness, we were able to show that behaviors perceived to be more serious would be less prevalent than those perceived to be less serious. Also e-mailing activities, such as receiving, checking and sending non-work related e-mails, were common and not really serious.

Second, we drew on previous research to examine how employees justified cyberloafing. Our results suggested that respondents were likely to provide excuses that trivialize, or downplay the consequences, arguing that the activities do not consume much time nor harm to the organization. Another common justification involved normalization—that if everyone else was cyberloafing. Not being treated fairly was another reason for cyberloafing.

Third, our findings also provided empirical evidence that the Internet made the boundary between work and home less distinct, shifting more work to home than personal errands to the workplace.

Fourth, this study conceptualized four key aspects of cyberloafing. The research framework can enable practitioners and researchers to better examine the various issues involved in understanding and dealing with cyberloafing.

Fifth, findings have provided insights on attitudes towards cyberloafing and how employees justify it.

7. Implications

Taken together our findings suggest that employees may believe that cyberloafing is justifiable. To this end, organizational efforts to keep it to a minimum should be directed toward neutralizing employees’ tendency to justify their behaviors. They also suggest a need for organizations to define and manage employees’ workplace Internet usage.

In principle, allowing employees the use of company Internet access for personal matters is not very much different than the traditional issue of allowing some “reasonable” amount of personal calls on the company telephone. In practice however, the Internet poses a much more sweeping opportunity for abuse. While some companies may decide that cyberloafing is acceptable, others may decide to prevent Internet access, or allow access but monitor the usage.
Regardless of the stance, there is a clear need for explicit guidelines. The policies may state what constitutes acceptable cyber activities, what means will be used to monitor employees’ use of cyberspace; and what disciplinary actions might be enforced. As such, it is imperative that such policies be communicated to all employees.

8. Limitations

Our study relied mainly on data provided by employees who had Internet access in their workplace. It is possible that organizational representatives responsible for developing policies may view the issue differently.

Second, our data were collected mainly using an online survey methodology. This may result in bias if respondents were also those self-selected as likely to cyberloaf. To mitigate such a problem, we compared the characteristics of our respondents with those of the typical Internet users in Singapore and found that they were not systematically different from the average Internet users in terms of age, educational level, and experience with Internet usage. However, we acknowledge that the current method of data collection is not totally foolproof.

Third, the current study did not distinguish between cyberloafing activities targeted at the organization versus those targeted at co-workers.

Fourth, organizational norms and social values could have an impact on what is considered “deviant behavior.” Further, from a country/national perspective, culture may have an impact on what is “acceptable” or “deviant.”

9. Conclusions

For most companies, the issue of what constitutes acceptable and unacceptable cyber behavior at work remains a gray area, an intricate matter that is subject to management and employees’ negotiation and perception.

This has led to much confusion among employees regarding management’s stance on cyber activities at the workplace. Clearly, management must develop clear acceptable Internet usage policies. While this may not eliminate all cyberloafing activities at the workplace, it would help make sure that employees understood the company’s stance.

Appendix A. Appendix: Instrument

A.1. Prevalence of cyberloafing

Scale: 0 (never), 1 (a few times/month), 2 (a few times/week), 3 (once a day), 4 (a few times/day), 5 (constantly).

During office hours, how often do you use the Internet at work to access the following Websites for personal reasons:

1. Visit non-job related Websites
2. Visit general news Websites
3. Visit entertainment-related Websites
4. Visit sports related Websites
5. Instant messaging/chat online (IRC)
6. Download non-work related information
7. Look for employment
8. Shop online
9. Play online games
10. Visit adult-oriented (sexually explicit) Websites
11. Check non-work related e-mail
12. Send non-work related e-mail
13. Receive non-work related e-mail

A.2. Perceived seriousness of cyberloafing items

Employees can use the company’s Internet facilities to engage in many different kinds of cyber activities during working hours at the workplace. Below is a list of these cyber activities.

Some are considered to be very serious, others not so serious, in terms of their consequences to the company (cost, time lost, productivity lost). We are interested in your opinion about how serious each type of cyber activity is.

If you think it is among the least serious, mark against the number 0 beside the cyber activity. If you think it is among the most serious, then mark against the number 5. If you think the cyber activity falls somewhere between the least serious and the most serious, then mark against the number between 0 and 5.
Remember that the seriousness of a cyber activity is only a matter of opinion, and it is your opinion that we want (scale: 0 (not at all serious), 5 (most serious)).

1. Visit non-job related Websites
2. Visit general news Websites
3. Visit entertainment related Websites
4. Visit sports related Websites
5. Instant messaging/chat online (IRC)
6. Download non-work related information
7. Look for employment
8. Shop online
9. Play online games
10. Visit adult-oriented (sexually explicit) Websites
11. Check non-work related e-mail
12. Send non-work related e-mail
13. Receive non-work related e-mail

A.3. Regulation of Internet

1a) Does your organization have policies regarding the use of the Internet?
   a) Yes        b) No        c) Don’t Know
b) If yes, please provide details.

c) Are these policies generally acceptable to you?
   a) Yes        b) No        c) Don’t Know

2) Do you know anyone, professionally or otherwise, who had been disciplined due to non-work related Internet usage at the workplace?
   a) Yes        b) No
If yes, please provide details:

3) Do you think it is acceptable to use the company’s Internet access for non-work purposes during working hours at the workplace?
   a) Yes        b) No
Please state some reasons for your response above.

4) Please provide some reasons/occasions when you feel that it is acceptable for employees to use the company’s Internet access for non-work purposes during working hours at the workplace?

5) I feel that it is acceptable for employees to use company’s Internet access for non-work purposes during working hours insofar as it does not exceed _____ minutes per day.

6) At home, I spent on average _____ hours per week on the Internet for work-related activities.

7) At work, I spent on average _____ hours per week on the Internet for personal activities.
References

[38] D. Verton, Employers ok with e-surfing, Computer world (34) 2000, pp. 1–16.
Vivien K.G. Lim is associate professor with the Department of Management and Organisation, NUS Business School. Her research interests include use and misuse of technology, job insecurity and job loss, workplace deviance and discipline, money ethic and workplace health issues. She has published more than 50 journal and conference papers. Her works have appeared in internationally refereed journals such as Communications of the ACM, Human Relations, Journal of Organizational Behavior, Journal of Vocational Behavior, Omega, Journal of Economic Psychology, Personality and Individual Differences, and Journal of Behavioral Medicine. Her research has also been featured in The Straits Times, Business Times and practitioner-oriented outlets such as Human Resource Review.

Thompson S.H. Teo is information systems area coordinator and associate professor in the Department of Decision Sciences at the NUS Business School. His research interests include the strategic uses of IT, e-commerce, adoption and diffusion of IT, and strategic IT management and planning. He has published more than 80 papers in international refereed journals such as Communications of the ACM, Database, Decision Sciences, Decision Support Systems, Information and Management, International Journal of Electronic Commerce, European Journal of Information Systems and Journal of Management Information Systems. He is also on the editorial board of several IS journals.