Information & Management 52 (2015) 170–182

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure

Jeremy Glassman, Marilyn Prosch, Benjamin B.M. Shao [*]

Department of Information Systems, W.P. Carey School of Business, Arizona State University, Tempe, AZ 85287-4606, USA

ARTICLE INFO

Article history:
Received 14 February 2014
Received in revised form 28 May 2014
Accepted 2 August 2014
Available online 12 August 2014

Keywords:
Cyberloafing
Internet filtering and monitoring
Agency theory
Operant conditioning
Procedural justice
Social norms

ABSTRACT

The goal of this study is to explore and analyze the effectiveness of a possible countermeasure to the so-called "cyberloafing" problem involving a technical solution of Internet filtering and monitoring. Through a multi-theoretical lens, we utilize operant conditioning and individuals' psychological morals of procedural justice and social norms to study the effectiveness of this countermeasure in addressing the associated agency problem and in promoting compliance with an organization's Internet usage policies. We find that in addition to the blocking module, confirmation and quota modules of an Internet filtering and monitoring system can prevent shirking and promote better compliance through employee empowerment and attention resource replenishment.

1. Introduction

Computers were initially created and used for primarily work-related functions. However, with the advent of the World Wide Web and ubiquitous computing, computers are also being used to engage in hobbies and to facilitate social connections. The use of web-enabled computing devices for both personal and business use has dramatically grown in recent years. Since computers and Internet access play an increasingly important role in the personal and professional lives of knowledge workers, the overlap between these two aspects has posed a serious issue for management across organizations [19].

In essence, the ubiquity of information technology (IT) and diffusion of the Internet have led to a prevalent mixture of personal and business Internet usage at work [4]. While users can access the Internet to complete their tasks more effectively, access to the Internet also increases the chance that they become distracted at work by engaging in activities such as shopping online, visiting news sites, emailing family and friends, or sharing pictures on social networks. This new type of loafing on the job has been coined as *cyberloafing* [25,26].

Muhl [31] found that in many organizations, management and employees have an implicit understanding that a certain amount of personal Internet usage is allowed at work. However, with the multitude of addicting Internet services such as social networks, games, and the ever-quickening news cycle [41], increasingly more employers are concerned that this "allowance" can be abused. Internet abuse by employees may affect organizations in several ways. For example, companies have to increase their IT expenditures, combat the exposure of their networks to potential threats, and monitor employee productivity more closely [34]. To reduce their exposure to these risks, organizations have adopted and implemented various control mechanisms, such as Internet usage policies [17] and software systems designed to block access to certain websites [38].

In a survey regarding compliance and enforcement of Internet usage policies [17], onerous web filtering rules and severe sanctions for non-compliance were found to have negative effects that are contrary to policymakers' intentions. Henle et al. [17] utilized personal norms to measure the likelihood of an employee to comply with Internet usage policies. They found that when facing increased severity of sanctions for non-compliance with Internet usage policies, employees with high personal norms were less likely to comply with the policies, while those with low personal norms were more likely to comply. Their finding suggests that effective solutions to cyberloafing need to be non-intrusive for employees who are more likely to comply with Internet usage policies but more direct for employees who are less likely to comply [28]. In addition, researchers in a cross-cultural study found that perceptions about the utilization and benefits of IT may affect employees' their usage of such technology [3].

[*] Corresponding author. Tel.: +1 480 727 6790; fax: +1 480 727 0881.
E-mail address: benjamin.shao@asu.edu (Benjamin B.M. Shao).

http://dx.doi.org/10.1016/j.im.2014.08.001
0378-7206/© 2014 Elsevier B.V. All rights reserved.

The possibility for Internet abuse reflects an agency problem where employees (agents) and an employer (principal) have incongruent goals. In this context, information asymmetry between employees and the employer exists because the employer is unaware of how employees utilize the Internet resources of the organization [20]. As with most agency problems, monitoring is a possible solution, for example, through the use of an Internet filtering and monitoring software package in this case. The goal of this study is to investigate the effectiveness of a countermeasure to cyberloafing involving prolonged exposure to a conditioned stimulus that reinforces the notion that excessive non-work-related Internet use at work is unacceptable.

Sales of Internet filtering software indicate that its popularity is continually rising, as the combined revenue of leading companies in the Internet monitoring and filtering industry in 2012 was estimated to be $1.18 billion by Gartner Reports [32]. From their analysis, the market grew approximately 15% from 2011 to 2012, and they anticipate that the market will grow another 13% to 15% in 2013. The leaders in the Internet filtering and security market are Websense, Cisco, McAfee, and Bluecoat Systems, among others. Within the web filtering industry, various types of filtering systems are available. Currently available Internet filtering systems are all capable of blocking access to sites that are placed on a black list and/or allowing access to sites placed on a white list only. Some Internet filtering systems also monitor and record all employee access to the Internet and produce reports for management. Previous research provides evidence that Internet filtering systems do not sufficiently address the underlying issues associated with abusive Internet access and that such systems also engenders a sense of employee resentment about potential surveillance from the enforcement of Internet monitoring and filtering [38].

The rest of this paper is organized as follows: In the next section, we discuss different types of Internet usage filtering software that are available on the market and review the related theories that can be leveraged to study the agency problem of cyberloafing in the workplace. We then examine the individual filtering modules of an industry-leading Internet filtering system, state the goal of each module for hypothesis formulation, and link each module to the associated theories. The filtering system that we describe has been operating in a mid-sized diversified company, and we examine the monitoring data gathered by the organization for hypothesis testing to study the effectiveness of different Internet filtering modules. Finally, we discuss the results, their implications for practice, and future research directions before we conclude the paper.

2. Theoretical foundation

Prior research has examined several potential methods to mitigate inappropriate Internet usage, including the establishment of Internet usage policies, training, and monitoring. Researchers have found that periodic monitoring through software that tracks Internet usage reduces cyberloafing [17]. In a laboratory experiment, employees who were informed that their Internet usage would be electronically monitored were more task focused, meaning that they engaged in less cyberloafing than employees who were monitored with no knowledge of whether the monitoring system was actually implemented and functioning [38]. Hence, an electronic monitoring system alone is not a perfectly effective solution and has to be supplemented by other methods. One method to increase employees' awareness of an electronic monitoring system is through an established corporate policy to inform them of the presence of such a system documented by their signature [42]. Another method, which we examine in this study, is the use of a filtering mechanism to establish awareness of this monitoring policy and deter inappropriate use through the prohibition of cyberloafing activities.

The extant research on the phenomenon of abusive Internet practices at work focuses on short-term experiments to determine how users respond to deterrence systems. By contrast, the goal of this study is to investigate prolonged exposure to a conditioned stimulus that reinforces the notion that excessive non-work-related use of the Internet is unacceptable at work. In most existing web monitoring software, this conditioning process involves a managerial role that requires employees' supervisors to act on the information generated from a report and to inform users of their acceptable or unacceptable behavior. Existing related research has followed this approach where users were notified of their monitored actions if they had abused their Internet access [38]. In essence, a system that reminds users that the site they are visiting has questionable work value every time they access it provides real-time feedback to employees. Furthermore, such a system serves another purpose of deterrence by dissuading employees from abusing their Internet access. In the following subsections, we review relevant theories that pertain to the explanation of cyberloafing and its potential avoidance. The theories include agency theory, operant conditioning, procedural justice, and social norms.

2.1. Agency theory

The basis of agency theory is a relationship between a principal and an agent who acts on behalf of the principal [20]. Such relationships are formed when the owner of resources (principal) hires another party (agent) to perform work. The most recognizable form of an agency relationship is that of an employer (principal) and employees (agents). While both parties work toward the same goal, they may not always share the same interests. A key element of an agency problem is goal incongruence where the goal of the agent is inconsistent with that of the principal. When an agreement is made through mechanisms such as a contract, the lack of perfect information about the goals and productivity of the agent can lead to information asymmetry and can create a monitoring problem whereby the principal cannot easily observe the agent's actions or verify the information provided by the agent without exerting substantial effort or incurring considerable costs [12]. Common methods to address agency problems are engaging in intensive monitoring of agents and creating effective incentives to foster appropriate behavior.

Researchers in the IS field have used agency theory to explore various agency issues. For example, Dawson et al. [10] studied the relationship between consultants and clients, and they noted that a limitation of the application of agency theory is that the theory espouses monitoring as the primary method of combating the issues. In some cases, the intrinsic complexities of a situation with necessary specialized knowledge diminish the effectiveness of monitoring efforts. However, in our study, the technology being examined is able to automatically and effectively monitor employees in a workplace setting without involving substantial human intervention.

Inappropriate Internet usage is a prime example of a principal-agent relationship where the core issue can be viewed as an agency problem. In other words, cyberloafing illustrates an agency problem when an employee (agent) is cyberloafing and when he/she is doing so against the wishes of the employer (principal). Viewed from the perspective of agency theory, cyberloafing occurs because many organizations do not seek to specifically address this particular agency problem and, as a