Organizational Aspects of Cyberloafing

Elisa Bortolani
University of Verona, Italy

Giuseppe Favretto
University of Verona, Italy

INTRODUCTION

The introduction of new technologies at workplaces causes the emergence of new organizational productivity threats. These threats are both inside and outside the organizations themselves. More often, organizations regret[1] programming and administrative errors; system and technical failures; sabotages; unauthorized accesses; disruption, manipulation, or loss of data and programs, not due to cyber-criminality (intrusions, employees' disloyalty, etc.); widespread virus; and issues caused by wireless devices. External threats, on the other hand, are more related to natural catastrophes (flooding, earthquakes, etc.), fires, industrial espionage, cyber-criminality, viruses, unfair competition, and physical damages to structures.

It is necessary for organizations to protect themselves from both intrusion attempts and employees' technology misuse. A United States survey[2] revealed that 35% of companies interviewed about suffered attacks in 2004 said that the prevalence was from insiders; on the other hand, only 26% revealed a prevalence of outsider attacks. Compared to the previous year, the trend was inverted. In 2003, in fact, insider attacks were around 14% and outsider attacks were about 23%. This, it is possible to think that insider threats will become more and more frequent and dangerous.

According to Radcliff (2004), internal data thefts are estimated to be 75% of total data thefts. An employee, for example, can copy and misappropriate a customer's database before passing it to the competitors. Another possible scenario is referred to as waste of efficiency caused by business e-mail abuse or Internet access misuse.

The FBI's Computer Crime Squad affirms that it is not necessary to blame corrupt or vindictive employees for all intrusion issues. Many problems, in fact, can be traced back to an improper use of IT business resources. Actually, for example, many companies that had put up with employees surfing the Internet for non-work-related activities for years now regretted Internet misuse, characterized by pornography, mp3, and illegal software downloading.

More than this, illicit software downloading and surfing insecure sites allow virus and malware introduction. This software, if installed on strategic machines, can make the company vulnerable. And so, costs are not limited to loss of business resources (e.g., working time), but are also related to damages caused by illicit and careless online employees' activities.

If, on one hand, the opportunity to work online helps in increasing several organizations' productivity (Anandarajan, Simmers, & Igbaria, 2000), on the other hand it causes an addition in number and level of risks. So, a lot of Internet access issues are related to information download (copyrighted software, offensive material, infected files, etc.), but the loss of productivity related to this habit does not seem secondary. In other words, without leaving their desks and without social control risk, the employees may, more easily than in the past, give themselves up to surfing the Net for non-work-related purposes.

Some years ago, a U.S. survey affirmed that 30-40% of daily business Internet traffic was attributed to surfing the Net for personal purposes.[3] In another research, carried out in 2001,[4] 51% of Italian employees affirmed access to non-work-related sites — more than English (44%), German (41%), and French (29%). And finally, another U.S. survey[5] shows that the average time spent online by respondents who admitted to using the Internet for personal purposes (58%) is about three-and-a-half hours per week.

Despite many people already having Internet access at home, about half of all online shopping and 70% of the global pornographic traffic[6] are registered during working time.[7] The favorite activities for surfing the Net are: holiday booking (52%), culture (42%), hobbies (41%), shopping (28%), sports (30%), and job searching.

The average user spends about two hours per day online, and 31% is for non-work-related surfing.[8] Seventy percent of employees admit either visiting "for adult" sites or sending personal e-mails during work time, 64% also send offensive or politically incorrect messages, and 57% admit surfing online decreases their own productivity.

A survey conducted in 2004[9] reports that of 3,245 respondents belonging to 750 employers, 40% answered to spending 40% of his or her working time cyberloafing, with an increase of one hour per day in the last year.

Organizational expenses in loss of productivity are estimated at billions of dollars per year (Greengard, 2000; Gordon, Loeb, Lucyshyn, & Richardson, 2005). After all, as evidenced by IDC Research (2000), U.S. and European Internet users seem to spend more time online when they are at work than when they are at home. This is probably due

to two characteristics of the workplace: perceived privacy and higher speed to link.

This new form of productive deviance, defined by Lim (2002) as *cyberloafing*, consists of business Net access during working time to surf for personal ends and/or to manage personal e-mails.

Siau, Nah, and Teng (2002) identify 11 categories of Internet abuses: general e-mail abuses, unauthorized usage and access, copyright infringement/plagiarism, newsgroup postings, transmission of confidential data, pornography, hacking, non-work-related download/upload, leisure use of the Internet, usage of external ISPs, and e-moonlighting (side jobs).

Especially, focusing on e-mails, Whitty and Carr (2006) affirm that cyberloafing is not always an intentional choice but sometimes is induced by other people. Ninety percent of their respondents, in fact, perceive chain e-mail, sent by friends or known people in any case, as more unpleasant than e-mail spam, and 17% perceive joke e-mails as objectionable. The modality to manage e-mails is increasingly an emerging issue and requires new and socially shared rules.

BACKGROUND

Lim (2002) categorizes cyberloafing as productive deviance (see Robinson & Bennett, 1995) but, for its consequences, it may also be included in:

- Property deviance (Hollinger & Clark, 1983);
- personal aggression (psychological harassment, e.g., sexual or racist e-mails); and
- political deviance, defined as the use of incorrect means to put someone at a political disadvantage in comparison with someone else (see Robinson & Bennett, 1995).

Mastrangelo (2002) suggests three dimensions below a counterproductive computer use. Each of them corresponds to the necessity of:

a. Social linking (personal e-mail, instant messaging, chat);
b. doing an errand; or
c. indecent behavior.

Lim (2002) proposes a cyberloafing explanation model starting from considerations about treatment equity (see Adams, 1965; Foa & Foa, 1976) and distributive justice (Deutsch, 1985; Skarlicki & Folger, 1997) in the organizations. She identifies in neutralization (Sykes & Matza, 1957) the theory construct to explain cyberloafing. Neutralization, in her opinion, is the individual attempt to rationalize a situation to convince himself and the others to be right and that deviant behavior is understandable. This mechanism of rationalization aims at building and preserving one's image.

Through neutralization, deviant behavior does not appear as a revenge to the employee. This feeling, in fact not acceptable for the person, is mediated from a rational explanation. After all, cyberloafing becomes a way to reestablish a trade-off in the person-organization relationship. Loss of equity (in terms of economic, relational, or symbolic treatment) is restored through a cyberloafing behaviour, so the individual feels rewarded for the time and energy he or she spent for the company that was not recognized.

Anandarajan et al. (2000), instead, describe both organizational and personal factors involved in Internet misused at work. They applied Fishbein and Ajzen's (1975) Theory of Reasoned Action (TRA) to Internet use at work. The authors affirm that the use of the Net is influenced by perceptions, personal attitudes, and social influences. TRA is extended by authors to the Technology Acceptance Model (TAM), which focuses on information technologies' perceived usefulness. In TAM, the factors that motivate a person to use a computer could be categorized into two groups: extrinsic motivators (perceived advantages, social pressure, etc.) and intrinsic motivators (playfulness, distraction, etc.). The proposed model shows four kinds of multidimensional variables. Research outcomes refer a more frequent, easier access and more time spent online by men than by women. Moreover, the ability to use the Internet and the Web are related to improvement in job characteristic perception (significance, autonomy, heterogeneity, job control, etc.). Playfulness can lead to perception of job characteristics improvement, more job satisfaction, and more global productivity. Actually playfulness, is a double-edged weapon; in fact, it can lead easily to Internet misuse with negative consequences in terms of increasing loss of time, necessity of redoing work because of a loss of accuracy, and a longer period of time in order to complete a task. These factors contribute to ineffectiveness and loss of productivity. On the other hand, social pressure and organizational support are associated to a kind of intimidation, which implies a lower use of the Internet. It suggests that management's commitment and support in the use of the Net can reduce the abuse. In addition, employees with high-structured tasks are less involved in improper use of the Internet at their workplace. The same result has emerged for people who have a low task variability. These considerations imply that employees with less structured tasks have a higher use of the Internet for personal scopes.

Henle and Blanchard (2005) suppose that, at first, employee cyberloafing is a modality of stress coping and that they do it only if the perception of sanctions by the organization is low. In fact, cyberloafing increases when there are no sanctions, but contrary to their initial expectations, it increases when workload is low.

It is interesting to quote the research of Lara, Tacoronte, and Din (2006). Their study shows that the variable leader