Computers in the workplace

Technology, Computer

Abstract

The discussion is centered on the non-business use of computers at workplace. The issue is considered through the technological prism, aimed at evaluating approaches towards its resolution and recommending an organizational policy to minimize negative consequences.

Computers in the Workplace

Thetechnological progresshas reached all spheres of corporate performance. Having initially been aimed at producing positive results for business entities, the use of technological solutions in the workplace seems to have brought significant amount of controversy and negativity into employer-employee relations. The dual character of using technologies in the workplace is seen in employees having free access to a wealth of information stored electronically; simultaneously, employers have the same access towards a wealth of tracking and monitoring techniques to minimize ‘ cyber slacking’ (or ‘ gold-bricking’). Internet connectivity and similar technologies are much owed for creating competitive corporate gains; but ‘ the Internet has quietly emerged as a playground for workers, who increasingly trade stocks, downloadmusic, - all during working hours’. (Doubilet & Polley, 2002, p. 11) In 2000 two-thirds of the American enterprises disciplined their employees for ‘ cyber slacking’; one third of U. S. firms have also terminated their workers. (Greengard, 2000, p. 2)

Obviously, business entities which do not possess and exercise sound technological policies face the highest risks of financial and related losses due to ‘ cyber slacking’. These technological policies represent corporate

legal instructions, which should clearly determine the limits of the employer’s and employee liability for technologies’ misuse in the workplace. For example, ‘ Chevron and Microsoft found themselves setting sexual-harassment lawsuits for $2. 2 million apiece as a result of internally circulated e-mails that, according to the law, might have created hostile work environments’. (Osmanoglu & Schramm, 2002, p. 123) The traditional e-mail tools used in business correspondence create serious business risks due to their ‘ impersonal’ character; the ‘ isolated’ email character frequently distracts the message’s author from thinking what was being written. Many enterprises take e-mails less formally than they have to. (Muhl, 2003, p. 14) Instant messaging is another risk faced by business organizations which do not realize potential seriousness of issues caused by employees’ using IM at work.

‘ For instance, most consumer-grade IM software (the type that is downloadable at no cost, which a vast majority of IM users use) does not have the capability to detect and filter out potentially harmful communications.’ (Ceniceros, 2004, p. 15)

Having once faced a serious technological threat, numerous enterprises conduct profound research and implement advanced technological solutions to monitor the use of e-mail and IM by employees; yet hardly many corporations view blogs as a potential threat to their business stability. The consequences of such blogging may be unpredictable. (Blakeley, 2003, p. 26) ‘ Blogs are created to continuously update a group of people or the public about the personal events in the blogger’s life’. (Muhl, 2003, p. 18) The unpredictability of of blogging is viewed through the risk of spreading

confidential commercial information, including the specific information about company’s partners or consumers. The fact is also that employees are distracted from productivity, accessing blogs during work day.

The approaches traditionally used by business organizations in order to put the discussed situation under control, are very controversial. This controversy is seen in involving the questions of privacy andhuman rightsinto the problem of corporate safety and confidentiality. Fifty-six percent of the U. S. enterprises state that they know employees, who use workplace technologies in private purposes. (Levine, 2005, p. 93)

The range of approaches towards decreasing and eliminating non-business use of technologies in the workplace is unlimited. However, employers should reasonably understand that non-businesstechnologyuse in the workplace cannot be 100% eliminated. The widely spread techniques of monitoring include video cameras and statistics of internet sites’ visitation. (Muhl, 2003, p. 18) Keystroke software is one of the most recent technological developments to be used for employees’ monitoring. GPS software is also frequently ‘ implanted’ into employer’s property, providing the employer with the opportunity to control each and every employee’s step. The so-called ‘ packet-sniffling’ software is a new instrument of supplying the employer with the information employees exchange in workplacecommunication. (Ceniceros, 2004, p. 17)

The advantages of these approaches depend on the level of technology sophistication, as well as its cost (or affordability). For example, VeriChip Corp. has supplied its employees with the chips implanted into their arms. The chips are integral to a radio-frequency identification system and allow

the employer to track each employee’s movement. The reason to use this technological solution is again anchored in the widely spread technologies’ misuse by employees. (Greengard, 2000, p. 4) These approaches seriously increase the tension between employers and employees, frequently being taken as the employee’s privacy breach.

A sound corporate policy should be designed to minimize the negative effects of ‘ cyber slacking’. The essential aspects to be included are: the limits of the permissible personal use of technologies in the workplace; confidential information aspect; communication standards; penalties; employee acknowledgement of the ‘ no privacy rights’ in the workplace. (Levine, 2005, p. 144) Accounting all these aspects will provide the company with the opportunity to prevent any technologies and information misuse in the workplace.

Conclusion

Using advanced technologies in the workplace creates bilateral effects: on the one hand, it is the direct pathway of business development in the contemporary world; on the other hand, the risks created by non-business use of these technologies threaten corporate safety and display alarming tendency towards technological negligence and misuse. Sound technological policies in combination with the use of monitoring techniques must be used to promote successful business performance; otherwise, the ‘ cyber slacking’ issue risks to acquire uncontrolled and comprehensive global character.

References

Blakeley, S. (2003, September). Reducing the risk of the errant e-mail with new technology:

Disappearing e-mail. Business Credit, 105 (8): 26

Ceniceros, R. (2004). Employees’ e-mails seen as posing professional liability risk. Business

Insurance, 38(50), 10-18

Doubilet, D. M. & Polley, V. I. (2002). Employee use of the internet and e-mail: model

corporate policy. Section of Business Law, American Bar Association.

Greengard, S. (2000). The high cost of cyber slacking – employees waste time online.

Workforce, December, 1-7

Levine, D. (2005). Reinventing the workplace: How business and employees can both win.

Brookings Institution.

Muhl, C. (2003). Workplace e-mail and internet use: employees and employers beware: An

employee's personal use of an employer's e-mail system and internet access is not protected under the law, and employers can face legal liability for employees' inappropriate use thereof. Monthly Labor Review, 126, 13-19.

Osmanoglu, T. E. ; Schramm, J. R. (2002). External data feeds: The new web of trust solves

some problems, but creates security vulnerabilities. Business Communications Review, 32 (January), 121-125

;