Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

12-31-2007

Managing the Dark Side of Computer Use at Work: A Typology of Information Technology Abuse and Management Strategy

Matt Campbell
University of North Carolina, Charlotte, smcampbe@uncc.edu

Ying Lu
University of North Carolina, Charlotte, ylu5@uncc.edu

MANAGING THE DARK SIDE OF COMPUTER USE AT WORK: A TYPOLOGY OF INFORMATION TECHNOLOGY ABUSE AND MANAGEMENT STRATEGY

Matt Campbell
University of North Carolina, Charlotte
smcampbe@uncc.edu,

Ying Lu
University of North Carolina, Charlotte
ylu5@uncc.edu

Abstract

With the myriad of computer-based information technologies available to businesses today, organizations face many challenges. One of the most crucial challenges is to prevent employees from abusing the technology provided to them in the performance of their jobs. Synthesizing and extending prior research, we propose a typology of Information Technology Abuse and Management Strategy (ITAMS). This ITAMS typology provides a useful guideline for managers to assess the status of technology abuse in the workplace and choose an effective strategy to deal with it, while reducing potential negative effects on employee productivity and morale.

Keywords: Information Technology Abuse and Management Strategy (ITAMS), Prevention, Deterrence, Acceptable Use Policies

Introduction

Computer-based information technology (IT) has significantly changed the way employees in many organizations accomplish their jobs. Although the use of information technology has many positive benefits, such as improving business processes, managerial decision making, and workgroup collaboration, there are also negative effects as well (O'Brian and Marakas 2005). Studies have found that employees abusing technology in the workplace can cause damage to the organization through loss of productivity, loss of confidential information, data and equipment damage, and exposure to civil and criminal liability (AMA 2005). The purpose of this study is to synthesize a comprehensive typology of Information Technology Abuse and Management Strategy (ITAMS) to guide managers in proactively dealing with technology abuse in the workplace.

In this paper, information technology abuse is defined as the personal use of a work computer that violates formal organizational policies or informal norms and generates potential legal or ethical consequences. Technology abuse behavior at work can be classified into four categories based on two dimensions: 1) nature of actions (legal, but unethical to illegal), and 2) level of user ill-intent (low to high). Managerial strategies for combating undesirable behavior can also be classified as either deterrence-based or prevention-based. Deterrence is defined as "a negative motivational influence," while prevention is defined as "the act of hindering or obstructing or impeding" (American Heritage Dictionary of the English Language 2003). Thus, the main difference between the two terms is that prevention decidedly stops or blocks a person from doing something while deterrence aims to influence a person's will against a certain decision.

Use of either approach can have negative consequences. For example, while almost all technology abuse committed with a PC could be prevented by securing that PC in a locked vault (a prevention-based technique), the use of the PC for legitimate work is prevented as well. Use of deterrence-based techniques such as employee monitoring can lead to a decrease in employee morale, an atmosphere of distrust, and even acts of sabotage (LaNuez and Jermier 1994; Vorvoreanu and Botan 2000; Sharma and Gupta 2003). Managers dealing with technology abuse must find a balance between the use of prevention-based techniques and the use of deterrence-based techniques that allows for the greatest amount of legitimate work to be done, while at the same time lowering the chances that the technology will be used for unacceptable purposes.

This paper is organized as follows: First, drawing upon prior research, we create a classification of technology abuse behaviors in the workplace (Table 1). Using that classification, we construct an ITAMS typology (Table 2). We then elaborate the types of technology abuse behavior at work and the respective suggested managerial strategies, both social and technical, for each quadrant of behavior in the typology. Next, we discuss the implications of the typology and how it can be used to help managers deal with the issue of technology abuse. Finally, we discuss possible directions for future research.

Technology Abuse in Organizations

Technology abuse can have consequences that range from minor decreases in individual productivity to major legal liability for the organization. Robinson and Bennett (1995) developed a topology of general deviant behavior in the workplace to gain a better perspective about the types of behavior involved and to motivate further research. They sorted deviant behavior according to level of seriousness (minor or serious) and locus of effect (organizational or interpersonal). We extend this research by creating a topology based on empirical data from prior studies that focuses specifically on technology abuse in the workplace. Robinson and Bennett's work grouped together numerous dimensions (covert/overt, unethical/ethical, and unintentional/intentional) into a single dimension which they labeled minor/serious. Like Robinson and Bennett, our classification considers the mindset of the abuser (level of ill-intent), but differs from theirs by also considering the consequences of the actions (nature of abuse).

Table 1: A classification of technology abuse behaviors at work

		Level of Ill-Intent	
		Low	**High**
Nature of Abuse	**Illegal**	B: Negligent use	D: Corrupt use
	Legal (but Unethical)	A: Nonproductive use	C: Counterproductive use

Viewing behaviors in this way allows us to better understand the motivations and mindset of the user. Understanding the user's mindset will allow us to craft the most effective managerial strategy to deal with the abuse.

Technology abuse in organizations is not a trivial problem. A study by Belanger and Van Slyke (2002) found that abuses such as excessive personal web usage among employees are prevalent, with employees spending an average of about 2 hours per day on non-work activities. This represents approximately 25% of the work day spent in abusing technology (Belanger and Van Slyke 2002). Employers are noticing the results of technology abuse. A survey developed by Robert Half International Inc. revealed that 55 percent of executives polled said employee use of the Internet for non-business purposes was hurting organizational productivity (Roman 1996).

Organizations, sometimes learning by trial and error, are taking action to deal with these technology abuses in the workplace. For example, a 2005 survey of managers conducted by the American Management Association (AMA) found that of the companies surveyed:

- 65% use software to block access to inappropriate websites
- 36% track employees' content, keystrokes and time spent at the keyboard
- 50% store and review employees' computer files
- 55% retain and review employee email messages

Of the organizations that do monitor their internet connections:

- 26% have terminated workers for misusing the Internet
- 25% have terminated employees for e-mail misuse

Determining the best way to deal with a particular type of abuse is important. Managers dealing with technology abuse must find a balance between the use of prevention-based techniques and the use of deterrence-based techniques that allows the greatest amount of legitimate work, while at the same time lessening the potential for the technology to be used for unacceptable purposes. Instead of using a "once size fits all" approach in dealing with technology abuse, managers should attempt to tailor their response to each type of abuse according to what research has found to be most effective.

The ITAMS Typology

In order to aid managers in targeting their strategy to each type of abuse, we propose a typology of Information Technology Abuse and Management Strategy (ITAMS) (table 2) based on the above classification of technology abuse behavior at work (Table 1).

Table 2: The ITAMS Typology

Nature of Abuse	**Illegal - Activities that expose the organization to civil and/or criminal liability.**	**B: Negligent Use** Example Behaviors: • Downloading illegal content • Making illegal copies of software • Sending sexually explicit jokes Suggested Response: <u>Deterrence</u> • Use Selective Monitoring	**D: Corrupt Use** Example Behaviors: • Computer hacking • Theft of confidential data • Viewing sexually explicit content Suggested Response: <u>Prevention</u> • Restrict Access
	Legal (but Unethical) - Activities that cause a loss of productivity.	**A: Nonproductive Use** Example Behaviors: • Using personal email or chat • Conducting personal business Suggested Response: <u>Deterrence</u> • Define Expectations (AUP) • Use Productivity Measurements	**C: Counterproductive Use** Example Behaviors: • Moonlighting (working on outside projects) Suggested Response: <u>Prevention</u> • Limit Privileges
		Low	**High**
		Level of Ill-Intent	

A: Nonproductive Use

Description of behaviors and consequences

The Nonproductive Use Quadrant of the ITAMS typology encompasses behaviors that result in a loss of productivity for the organization, but are usually committed with a low level of ill-intent by the user. Previous research has suggested these abuses should be dealt with using a policy of deterrence. Activities in this quadrant include sending and receiving personal email (either through webmail or using the company email system for personal messages), chatting online, and conducting personal business online (i.e. buying stocks or paying bills). A number of studies indicate that activities in this category can result in a loss of productivity, a reduction in organizational resources, and an increase in labor costs (Anandarajan et. al. 2006). Research has found that inappropriate Internet usage by employees can result in productivity losses of 30-40% (Lim et. al. 2002) Ramayah and Baharudin (2005) conducted a study of personal web use during work hours and found that personal downloading, personal information research, and personal e-commerce were all linked to work inefficiency. Besides wasting employee time, these activities can also consume bandwidth which hinders others conducting legitimate work (Baharudin et. al. 2005). In addition to wasting company resources, inappropriate internet usage in this category can also expose the company to viruses and hackers who gain access through vulnerabilities exposed through the use of personal email (Lim et. al. 2002).

Not all consequences of this category of behavior are negative. Anandarajan et. al. (2006) notes that because of changes in family structures of the workforce, composition of work force, social structures, and gender roles; the use of the Internet during work hours can help to achieve a work-life balance for some employees. This balance, they claim, can affect personal and organizational wellbeing in positive ways. Research suggests that banning personal web usage altogether can have detrimental effects on employee productivity and morale. Anandarajan et. al. (2006) found that personal web usage could have a significant influence on job satisfaction. Berger and Van Slyke (2002) present the idea that a moderate amount of playful use of computer applications can aid in learning, which is a benefit to the organization. Stanton's (2002) research reveals that frequent Internet users tend to be happy and productive workers and Oravec (2002) presents the argument that the constructive use of technology for recreation can help the organization work harder and play better.

Suggested managerial strategy

Because of the lack of nefarious intent behind the behaviors in this quadrant, the suggested managerial responses in this category are some of the easiest and least expensive to implement. Four actions recommended by research to counter behavior in this quadrant are: 1) to use a strongly worded acceptable use policy followed up by punishment for violations, 2) to foster a corporate culture that does not support technology abuse, 3) to treat employees fairly and provide adequate compensation, and 4) implement productivity measurements.

A number of research articles promote the use of a well-developed, clearly articulated acceptable use policy (AUP) for employees. In addition, organizations must make sure that they communicate this policy to their employees so that employees will not violate it due to ignorance (Woon and Pee 2004; Lim 2002; Lim et. al. 2002; Ramayah and Baharudin 2005; Anandakajan 2002; Wen and Lin 1998; Sharma and Gupta 2003-2004; Belanger and Van Slyke 2002). When creating an acceptable use policy, there are a number of elements an organization should address:

- What is an acceptable amount of time to be spent on line for work related activities (Wen and Lin 1998).
- What is an acceptable amount of time to be spent on line for non-work related activities (Lim et. al. 2002; Siau et. al. 2002; Wen and Lin 1998).
- What material is acceptable to be viewed and what is not (Siau et. al. 2002, Ramayah and Baharudin 2005; Wen and Lin 1998).
- Guidelines for downloading from the Internet (Wen and Lin 1998).
- Guidelines for Chat Room Use (Wen and Lin 1998).
- When during the day should employees use the internet in order to avoid bogging down the system (Wen and Lin 1998).
- Guidelines for sending and receiving email (Wen and Lin 1998).
- What, if any, means of monitoring will be used (Lim et. al. 2002; Siau et. al. 2002; Wen and Lin 1998; Simmers 2002).

Once the AUP is completed, organizations must decide on how to inform end users of the policies and how to alert them to changes (Lim 2002; Wellen 2004; Siau et. al. 2002; Wen and Lin 1998; Simmer 2002). In addition, organizations should make sure that they enforce effective and consistent discipline for violations of the AUP (Woon and Pee 2004; Lim 2002; Wellen 2004; Siau et. al. 2002; Wen and Lin 1998; Simmers 2002). Few things will encourage employees to violate company policy more than seeing fellow employees committing violations without being punished. (Lim et. al. 2002).

Creating a corporate culture that encourages employees to act ethically has also been identified in the literature as a way to deter technology abuse (Gelletta and Polak 2003; Chang 1998). The three main actions needed to create this culture are to foster trust between employees and management, to promote employee belief that abuse of technology is bad, and to provide for the social and physical needs of employees. By creating a relationship of trust and commitment between employees and management, research suggests that organizations are able to create a buffer between individuals who abuse technology and others who may be influenced by their actions. This may be due to the fact that individuals who are more committed to the organization are more resistant to the temptation to abuse technology (Wellen 2004; Sharma and Gupta 2003-2004). Research suggests a healthy relationship between employees and management can also lessen the ability of employees to rationalize technology abuse (Wellen 2004). In addition, some studies have found that the most significant factor in an employee's decision to abuse technology is the influence of friends, families, coworkers and the organization's IT department (Woon and Pee 2004). Therefore, creating an organizational culture that discourages abuse is an effective way of influencing employee behavior against technology abuse. Organizations should also work to form beliefs in employees that abuse of technology is morally wrong. Research suggests that when organizations are able to attach a negative social image to an activity or induce guilt or shame in an offender, the chances of the employee committing that behavior are lessened (Wellen 2004, Annandarajan et. al. 2006). By changing the perception of technology abuse in the minds of employees, organizations can positively control technology abuse without reducing the employee's ability to accomplish work tasks.

Treating employees fairly and providing adequate compensation has also been identified in the literature with reducing employee abuse of technology and other undesirable behaviors. Lim (2002) suggested that the more individuals believed that their workplace was unjust, the more likely they are to rationalize the act of technology abuse. Lim found that organizations that are "distributively, procedurally and interactionally unjust in their treatment of their employees" have employees who are more likely to rationalize their abuse of technology as a justified response. Lim suggests that organizations can reduce the occurrence of employees rationalizing abusive behavior by treating them fairly and insuring that the workplace is conducive to good work practices. Inadequate compensation also was shown to play a role in technology abuse. Greenberg and Scott (1996) found that employee theft was a common response to inadequate pay. Lim et. al. (2002) found that when organizations overwork their employees and don't compensate them adequately, most individuals were not apposed to some forms of technology abuse. Therefore, organizations should adequately measure contributions of employees and make sure that they are compensated fairly. Compensation does not always need to take the form of additional pay. It could be accomplished through the use of "comp time" or even non-monetary awards or recognition of an employee's hard work.

Given the necessity of the Internet for employees to do their jobs, the contribution that personal web usage can make to work-life balance, and other positive effects; how can managers make sure that their employees are not abusing their access to the internet? Other suggestions have even included ideas such as providing employees with a home internet connection at the company's expense to allow them an opportunity to use the Internet other than at work (Sharma and Gupta 2003-2004).

While some organizations have responded by blocking all sites that are not deemed to be work related, blocking sites that are not pornographic, dangerous, or illegal in nature can have negative consequences. Employees will occasionally have a legitimate work-related need to access these sites. In addition, the number of sites that fall into this category is increasing every day, which makes trying to compile a comprehensive list impossible. Research has also indicated that some employees view non-work-related use of the Internet as a fringe benefit that can help relieve work stress (Woon and Pee 2004; Sharma and Gupta 2003). Research by Woon and Pee (2004) suggests that a better way to ensure the responsible use of the Internet for sites that fall into this category is to implement productivity measurement. This allows employees the freedom to view sites that are not pornographic, dangerous, or illegal in nature even for occasional personal use while still making sure that work is done.

B: Negligent Use

Description of behaviors and consequences

The Negligent Use Quadrant of the ITAMS typology encompasses behaviors that expose the organization to possible civil and criminal liability, but are usually committed with a low level of ill-intent by the user. Previous research has suggested these activities should be dealt with using deterrence. Activities in this category include downloading illegal copies of software, music, or movies from the Internet, making illegal copies of software owned by the organization, and sending sexually explicit messages or jokes via email.

Companies such as Chevron and Microsoft have both settled sexual-harassment lawsuits for $2.2 million apiece as a result of sexually related internally circulated e-mails that created hostile work environments (Conlin 2000). The Motion Picture Association of America has also sent out a warning to organizations alerting them to the fact that they can be held liable for their employees' illegal downloading over corporate networks (Naujeck 2003). Research has found that abuses in this category not only leave a company liable when employees make illegal copies of company software for friends or download illegal copies of software, but also hurt an organization due to a reduction in the availability of organizational resources. The transfer of large non-work related files can jam corporate networks causing a slowdown for legitimate users (Baharudin et. al. 2005). One study found that Napster, a file sharing site that allowed users to share copyrighted material, took up over 80% of available bandwidth at some of the organizations studied (Conlin 2000). In addition, this behavior also exposes the company network to the possibilities of viruses and hackers (Lim et. al. 2002).

Suggested managerial strategy

Because of the civil and criminal implications of these activities, the literature tends to support stronger methods of deterrence to control them than for activities categorized in the Negligent Use Quadrant. Seale (1998) and Taylor and Shim (1993) found that an employee's knowledge of the employer's software policies did not seem to influence reported piracy. In addition, Reid et al. (1992) found no connection between an employee's awareness of copyright law and unauthorized copying. Many organizations monitor employees' actions, however, because of problems associated with monitoring detailed by Urbaczewski and Jessup (2002), such as negative employee perceptions of monitoring, its detrimental effect on employee morale, and the costs of analyzing large numbers of log files, monitoring should be used sparingly.

Monitoring exists on many different levels. Software is available that allows management to monitor every single keystroke an employee makes. Most research does not advocate monitoring at that level for activities in this quadrant. Wen and Lin (1998) mention that Internet monitoring can track an employee's Internet movements and report on them, but point out that it can be very labor intensive to analyze the large amounts of data produced. Stanton (2002), speaking from an agency theory perspective, believes that monitoring may be necessary for workers with no strong stake in the organization such as temporary workers, but believes monitoring is likely to be counterproductive and irrelevant for employees who identify closely with the organization's values and whose professional goals are aligned with organizational goals. LaNuez and Jermier (1994) found that electronic control systems such as surveillance can result in a feeling of diminished control among employees that can lead to acts of sabotage by employees. Vorvoreanu and Botan (2000) found that negative affect (a negative feeling) is also a consequence of monitoring. Sharma and Gupta (2003) note that in some cases monitoring employees for Internet usage has resulted in lawsuits between employees and employers. Their research indicated that employer surveillance takes a physical as well as an emotional toll on employees. The effects of monitoring can actually result in a decrease in productivity. At the very least, monitoring employee Internet usage has created a good deal of mistrust between employers and employees and also brought a new level of suspicion into the workplace (Sharma and Gupta 2003).

To use monitoring sparingly and most effectively, it should be implemented as exception reporting and only in certain areas such as bandwidth usage, email keywords, and users who have already been observed abusing Internet privileges (Urbaczewski and Jessup 2002). Bandwidth monitoring will allow management to look at employees who are consuming large amounts of bandwidth as a legitimate business concern while not making employees feel that every move they make is being watched. Monitoring email for keywords that would indicate transmission of organizational secrets or inappropriate sexual content would again allow management to deter information theft and misbehavior as a legitimate business concern while not making employees feel that every email they send is being read by management. Reducing unnecessary access to and monitoring the use of company owned software installation disks can reduce piracy of company owned software (Chang 1998). Panko and Beh (2002) note the effectiveness of monitoring employees for pornography viewing and sexual harassment as long as it is done in conjunction with an acceptable use policy stating such monitoring will be taking place.

C: Counterproductive Use

Description of behaviors and consequences

The Counterproductive Use Quadrant of the ITAMS typology encompasses behaviors that result in a loss of productivity for the organization and are usually committed with a high level of ill-intent by the user. Previous research has suggested these behaviors should be dealt with using a policy of prevention. Activities in this quadrant include moonlighting (working on outside projects during work time).

Employees may engage in these types of activities as a means of generating additional income or just to satisfy an entrepreneurial spirit. Quite frequently, the offenders in this category are programmers, system analysts, and those with other high demand skills (Siau et. al. 2002). The main effect of this behavior is the lack of productivity caused by the employee's divided attention and commitment.

Suggested managerial response

Research suggests that a practical step that organizations can take to deter the practice of moonlighting is to use a security policy on the local machine to limit software installation to approved packages only (Schuff and Louis, 2001). Organizations can also install programs such as TIVOLLI or IBM Director to detect unauthorized software and files which exist on users' PCs (Baharudin et. al. 2005).

D: Corrupt Use

Description of behaviors and consequences

The Corrupt Use Quadrant of the ITAMS typology encompasses behaviors that expose the organization to possible civil and criminal liability as well as substantial loss through theft or intrusion and are usually committed with a high level of ill-intent by the user. Previous research has suggested these behaviors should be dealt with using prevention. Activities in this quadrant include viewing sexually explicit images or videos, computer hacking, unauthorized access, theft of confidential organizational information, and theft of physical organizational property.

According to Boston (2000), most serious computer breaches are perpetrated by a company's own employees. The effects of a computer breach on an organization's public image and stock price can be very expensive. A 2005 survey by the CSI/FBI reported that the 639 organizations that responded to the survey reported suffering $130 million in financial losses because of computer security breaches (Computer Security Institute 2005).

Suggested managerial strategy

One of the best ways to prevent abuse from activities in this category is to prevent unauthorized users from gaining access to network resources. Limiting the access to confidential information only to the employees who need it to do their jobs and blocking all others (Sandhu and Samarati 1994) will keep other employees and those outside the company from misusing that information. Restricting access can be done using identity verification technology such as passwords, tokens, or biometrics (Sandhu and Samarati 1994). Identity verification technology works by identifying each unique user and then allowing him or her to access only the resources to which they have been approved. But in order for this system to be effective, the organization must force users to choose sophisticated passwords, carefully guard their passwords, and make sure not to leave their computer unattended when they are logged in (Baharudin et. al. 2005). Finally, to guard against individuals who might try and take advantage of vulnerabilities in the system to gain access, organizations should implement intrusion prevention software (Frincke 2000). In order to reduce the opportunity presented by vulnerabilities present in any software the company is using, administrators should keep up to date with all security updates and patches once the patches have been tested and deemed compatible with the organization's current computer configuration (Baharudin et. al. 2005).

Some actions of individuals who are legitimate users of the system also need to be controlled. Most research does not advocate totally unrestricted Internet access within an organization. Some sites pose enough danger to the organization that they justify the total blocking of their use. Research suggests the use a firewall to deny access to sites known to feature undesirable or illegal content and to restrict external access to the company network. Through the use of applications such as Websense, organizations can block all identified undesirable sites. Use of such software helps reduce the risk of legal liability because it demonstrates that the organization has taken appropriate means to block such content in the company (Wen and Lin 1998). However, these applications can only prevent access to sites that have been identified as inappropriate which leaves newer unidentified websites accessible (Baharudin, et. al. 2005).

Discussion and Future Research

Organizations must take a proactive approach to dealing with technology abuse by their employees. Attempts to control technology abuse without first understanding the nature of the abuse and the intent of the abuser can result in an inefficient or possibly ineffective response by management. While, on the surface, it may appear most effective to block all undesirable activities, research has shown that this approach can often backfire and lead to more problems. Selective use of both deterrence and prevention-based strategies, as prescribed by the proposed topology, will allow managers to reap the rewards of new technology without experiencing many of the drawbacks associate with technology abuse.

Although the ITAMS typology is based on prior research, further testing is needed to verify that our classification of technology abuse behaviors at work is a valid interpretation of these studies. Future research could make use of qualitative techniques such as interviews to get a better understanding of employee motivations. Surveys to discover best practices in use in industry could also be valuable. This understanding would result in a more finely-tuned instrument for determining management strategy in dealing with technology abuse.

This paper has cited several studies that have examined different deterrence and prevention techniques, but more research is needed to understand the longer term effects of such policies on employees. For example, social research of prison inmates has shown that while new inmates may find the restrictions of life behind bars very hard to cope with at first; over time, they tend to become "institutionalized" and adjust to a point where they cannot function without a high degree of structure (Goodstein 1979). It is too early to tell if this process might be mimicked in information workers subjected to extreme implementations of deterrence and prevention policies in their workplaces. It would also be necessary to look at what such experiences do to an employee's level of creativity and ability to work autonomously.

Conclusion

In this paper, we propose a typology of technology abuse based on type of abuse and abuser intent. The goal of this paper is to present the idea that technology abuse is a multidimensional construct that must be understood in depth before it can be dealt with effectively. It is also our intention to help researchers identify areas where gaps in research exist as to the best way to counter specific undesirable behaviors by employees.

For managers dealing with technology abuse, it is imperative to find a balance between the use of prevention-based techniques and the use of deterrence-based techniques that allows the greatest amount of legitimate work, while at the same time, lowering the chances that the technology will be used for unacceptable purposes. While achieving this balance is difficult, the need to efficiently and effectively manage technology use inside the organization will become even more important as organizations use these tools to compete in an increasingly competitive marketplace. We believe that our typology will be a useful tool for practitioners formulating a response to technology abuse.

References

AMA/ePolicy Institute Research. 2005 ELECTRONIC MONITORING and SURVEILLANCE SURVEY. Online: http://www.amanet.org/research/pdfs/EMS_summary05.pdf

American Heritage Dictionary of the English Language, Fourth Edition, 2000, 2003. Houghton Mifflin Company. Online: http://www.thefreedictionary.com, 2003.

Anandakajan, M., "Internet Abuse in the Workplace," Communications Of The ACM (45:1), January 2002.

Anandarajan, M., Paravastu, B., and Simmers, D. "Perceptions of Personal Web Usage in the Workplace: AQ-Methodology Approach," Cyberpsychology and Behavior (9:3), 2006.

Baharudin, S., Zainuddin, Y. and Ramayah, T. "Computer Abuse in Public Work Places: A Case Study of A Malaysian Public University," The Journal of Accounting, Management, and Economics Research, (5:1), 2005, pp 91-99.

Balkovich, E., Bikson, T. and Bitko, G. 9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace TR-197-RC, 2005, 36 pp., ISBN: 0-8330-3719-6.

Belanger, F. and Van Slyke, C. "Abuse or Learning?," Communications Of The ACM (45:1), January 2002.

Boston, Terry. "The Insider Threat". October 24 2000. Online: http://www.sans.org/rr/securitybasics/insider_threat2.php

Case, C. and Young, K. "Employee Internet Management: Current Business Practices and Outcomes," CYBERPSYCHOLOGY and BEHAVIOR (5:4), 2002.

Chang, M. "Predicting Unethical Behavior: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior," Journal of Business Ethics, (17), 1998, pp. 1825- 1834.

Conlin, M. "Workers, surf at your own risk," Business Week Online, June 12, 2000. Online: www.businessweek.com/2000/00_24/b3685257.htm.

Cooper, A., Golden, G., and Kent-Ferraro, J. "Online sexual behaviors in the workplace: How can Human Resource Departments and employee assistance programs respond effectively?" Sexual Addiction and Compulsivity, (9), 2002, pp. 149-165.

Computer Security Institute, 2005 CSI/FBI Computer Crime and Security Survey. Online: http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

Frincke, D. "Balancing Cooperation and Risk in Intrusion Detection," ACM Transactions on Information and System Security, (3:1), February 2000, Pages 1–29.

Galletta, D. and Polak, P. "An Empirical Investigation of Antecedents of Internet Abuse in the Workplace," AIS SIG-HCI Workshop, Seattle, December, 2003.

Goodstein, L. "Inmate Adjustment to Prison and the Transition to Community Life," Journal of Research in Crime and Delinquency, Vol. 16, Jul 1979, pp. 246 - 272.

Greenberg, J., and Scott, K. "Why do workers bite the hand that feeds them? Employee theft as a social exchange process," B. M. Staw and L. L. Cummings (Eds.), Research on organizational behavior, (18), pp. 111-156, Greenwich, CT JAI Press. 1996.

Hollinger, R. and Clark, J. "Formal and informal social controls of employee deviance," Sociological Quarterly, (23), 1982, pp. 333-343.

LaNuez, D., and Jermier, J.M. "Sabotage by managers and technocrats: Neglected patterns of resistance at work," In Jermier, J.M., Knights, D., and Nord, W .R. (Eds.). Resistance and power in organizations (pp.219-251). London, New York : Routledge. 1994.

Lim, V. "The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice," Journal of Organizational Behavior, (23), 2002, pp. 675-694.

Lim, V., Teo, T. and Loo, G. "HOW DO I LOAF HERE? LET ME COUNT THE WAYS," Communications of the ACM, (45:1), January 2002.

Martzahn, T. "Implementing the 'Just-enough Privilege' Security Model," SANS Institute, Information Security Reading Room, August 22, 2003. Online: http://www.sans.org/rr/papers/56/1256.pdf

Mangione, T. and Quinn, R. "Job Satisfaction, counterproductive behavior, and drug use at work," Journal of Applied Psychology, (1), 1974, pp. 114-116.

Naujeck, J. "Bosses warned that workers' downloads can carry high costs," USAToday.com (February 2, 2003). Online: http://www.usatoday.com/tech/news/2003-02-21-downloads-work_x.htm

O'Brian, J. and Marakas, G. Chapter 1 (p. 4) in Management Information Systems. McGraw-Hill/Irwin; 7 edition. January 14, 2005.

Oravec, J. "Constructive Approaches to Internet Recreation in the Workplace," Communications of the ACM, (45:1), January 2002.

Panko, R. and Beh, H. "Monitoring for pornography and sexual harassment," Communications of the ACM, (45:1), January 2002.

Ramayah, T. and Baharudin, A. "Personal Web Usage in the Work Place: Results from a Preliminary Study," INCOMT 2005, Managing Future Workplace Issues and Challenges in the Borderless World. July 2005.

Robinson, S. and Bennett, R, "Typology of Deviant Workplace Behaviors: A Multidimensional Scaling Study" Academy of Management Journal Vol., (38: 2), pp. 555-572, 1995.

Roman, L. "Survey: employees traveling in cyberspace while on the clock," Memphis Business Journal, 1996, pp. 2-3.

Sandhu, R. and Samarati, P. "Access Control: Principles and Practice," IEEE Communications, September 1994, pp. 2-10.

Schuff, D. and St. Louis, R. "Centralization vs. Decentralization of Application Software," Communications of the ACM, (44:6), June 2001.

Seale, D., Polakowski, M., Schneider, S. "It's Not Really Theft!: Personal and Workplace Ethics that Enable Software Piracy," Behaviour and Information Technology, (17:1), 1998, pp. 27-40.

Sharma, S. and Gupta, J. "Improving Workers' Productivity and Reducing Internet Abuse," Journal of Computer Information Systems, Winter 2003-2004.

Simmers, C. "Aligning Internet Usage With Business Priorities," Communications of the ACM, (45:1), January 2002.

Siau, K., Nah, F., and Teng, L. "Acceptable Internet Use Policy," Communications of the ACM, (45:1), January 2002.

Stanton, J. "Company Profile of the Frequent Internet User," Communications of the ACM, (45:1), January 2002.

Urbaczewski, A. and Jessup, L. "Does Electronic Monitoring of Employee Internet Usage Work?," Communications of the ACM, (45:1), January 2002.

Vorvoreanu, M. and Botan, C. "Examining Electronic Surveillance In The Workplace: A Review Of Theoretical Perspectives And Research Findings," CERIAS Tech Report 2000-14, 2000.

Wellen, J. "From individual deviance to collective corruption: A social influence model of the spread of deviance in organizations," Social Change in the 21st Century Conference, Queensland University of Technology, Brisbane, 2004.

Wen, H. and Lin, B. "Internet and employee productivity," Management Decision, (36:6), 1998, pp. 395–398.

Wheeler, H. "Punishment theory and industry discipline," Industrial Relations, (15), 1976, pp 235-243.

Woon, I. and Pee, L. "Behavioral Factors Affecting Internet Abuse in the Workplace," Proceedings of the Third Annual Workshop on HCI Research in MIS, Washington, D.C., December 10-11, 2004.

Wyatt, K. and Phillips, J. "Internet Use and Misuse in the Workplace," Proceedings of OZCHI 2005, Canberra, Australia, November 23-25, 2005.