Gadjah Mada International Journal of Business
May 2004, Vol. 6, No. 2, pp. 193—224

INTERNET ACCESS PRACTICES AND EMPLOYEE ATTITUDES TOWARD INTERNET USAGE POLICY IMPLEMENTATION IN SELECTED PHILIPPINES FINANCIAL INSTITUTIONS

Maria Sagrario R. Simbulan

This study explores the employees' concept of appropriate use of Internet facilities as well as their perception of the rights and liabilities, both of the individual and of the organization, associated with the grant of Internet access privileges in the workplace. It further examines how employees perceive their organization's monitoring of employees online activities and the use of an Internet Usage Policy, whether these are seen as monitoring and control mechanisms or as ways to ensure that Internet access facilities are shared equitably and used responsibly. While the issue of the impact of Internet access on employee productivity will not directly be tackled, the study will provide insights into the frequency and type of usage of Internet facilities in the workplace. Considering the sizeable investment that an organization makes to provide Internet facilities, determining how employees use these facilities to achieve the goals of the organization is, in the very least, interesting and for most organizations concerned with their survival in difficult times, critically important.

Keywords: acceptable use policy; appropriate use policy; AUP; internet use policy; IUP; internet access rights; internet access monitoring

Introduction

In an increasingly digital world where great value resides in information and information systems, management's lack of awareness of the risks to the organization's information resources may lead to the destruction or theft of critical data with, of course, its attendant financial consequences. There are many ways that this can happen: by the introduction of viruses, through unauthorized access to and tampering with data. It is the increasing incidence of crimes involving the use of computers to steal, tamper with, misuse or otherwise compromise information resources and computing facilities that has prompted many organizations to adopt Acceptable Usage Policies (AUPs) in an effort to monitor, control and secure these resources.

The basic premise of any AUP is that the electronic information environment is provided to support the business of the organization and its mission. Other uses are secondary. Uses that threaten the integrity of the system, the function of equipment located outside the premises of the organization that can be accessed through the system, the privacy or actual or perceived safety of others, or uses that are otherwise illegal are forbidden (Carliner 1999).

What is an AUP? The AUP is a formal or informal document that defines the intended use of the organization's computing facilities and information resources, unacceptable uses, and the consequences for non-compliance (TechWeb 2004).

There are different types of AUPs from a resource management point of view. Some examples are: AUPs that deal specifically with the use of and access to information resources like digital files and databases; AUPs that cover the use of computing resources, specifically the disposition and allocation of hardware, and the use and installation of software; and AUPs that cover the use of network facilities, internet access and email. This type of AUP dealing with Internet-related resources, also known as an Internet Usage Policy (IUP), is the focus of this research paper.

Regardless of the type, AUPs are created with three goals in mind. *First*, to educate the members of the organization about activities that may be harmful to the organization. *Second*, to provide a legal notice of unacceptable behavior and the penalties for such behavior. *Third*, to protect the organization from liabilities arising from employees' use or misuse of Internet access facilities (Standler 2002).

Unlike financial organizations in the more developed countries, most Philippine banks and financial institutions do not grant every employee access to its Internet facilities for bandwidth and I.T. infrastructure cost-related reasons. The challenge, therefore, for managers is to ensure that all members of the organization who need Internet access in the performance of their jobs are able to do so without having to compete aggressively with others for access time or bandwidth. In organizations where bandwidth is limited, knowing how as well as how frequently employees use internet facilities at work will allow decision makers and planners to project future growth and demand for online access. The equitable distribution of this valuable but necessarily limited organizational resource is one of the reasons for the creation and adoption of Internet Usage Policies in organizations.

IUPs are verbal or written agreements all parties on a network or organization promise to adhere to for the common good. A well-written IUP will include provisions for network etiquette, limits on the use of network resources, and clear indications of the level of privacy a user of the network should expect (TechWeb 2004).

The study will explore the employees' concept of appropriate use of Internet facilities as well as their perception of the rights and liabilities, both of the individual and of the organization, associated with the grant of Internet access privileges in the workplace. The results obtained would help managers understand the concerns of their employees, particularly with regard to sensitive issues like access control and monitoring, privacy, and ownership of correspondence.

This study will look at two methods that organizations use as mechanisms to govern the use of Internet facilities in the workplace and examine the attitudes of employees toward these controls. These methods, the monitoring of employees online activities and the use of an Internet Usage Policy, can be perceived negatively as control mechanisms or positively as a way to ensure that Internet facilities are shared equitably and used responsibly. Knowing how employees perceive management efforts at maximizing available Internet infrastructure and bandwidth will help managers address sensitive issues like privacy, propriety, and harassment in the workplace.

This study will provide insights into the frequency and type of usage of Internet facilities in the workplace. Managers may find these insights useful, particularly in the crafting of IUPs (or revisions to existing ones) and in planning for future I.T. infrastructure investments. Knowing how employees use Internet access facilities at work will allow managers to determine the type of monitoring and control mechanisms that need to be instituted, as well as the content and 'tone' of the IUP. In organizations where employees are prone to abuse Internet facilities, a stronger and more proactive approach to monitoring and control will need to be reflected in the organization's IUP.

Considering the sizeable investment that an organization makes to provide Internet access facilities at work, determining how employees use these facilities to achieve the goals of the organization is, in the very least, interesting and for most organizations concerned with their survival in difficult times, critically important.

Literature Review and Hypothesis Development

Internet and Productivity

Several studies on Internet and productivity have been made showing conflicting results. A study by Oliner and Sichel (2000) found that the Internet had no impact on productivity, while Litan and Rivlin (2001) found the Internet's contribution to productivity growth to be .204 percent per year over the last half of the 1990s.

A study by Goss (2001) looked at the impact of Internet usage by industry over a 3-year period (1997 to 1999). Goss' results suggest that job-related Internet usage had a positive and statistically significant impact on productivity growth of .25 percent per year.

An Internet-based survey on Internet Use in the Workplace conducted by Vault.com (2000) again gave conflicting results: From the point of view of employees, only 33.4 percent agreed that surfing the Net or sending non-work-related emails decreased productivity. From the point of view of employers, however, a full 49.8 percent or half of the respondents thought that it compromised employee productivity.

Some numbers: A Harris Interactive survey of 305 employees in 2002 noted that the average worker spends more than one entire day each week surfing Web sites that are not work-related (Hyman 2002). In monetary terms, a study conducted by Websense, Inc. in 2002 showed that Internet misuse costs U.S. companies more than $85 billion annually in lost productivity. That estimate showed a 35 percent increase from the previous year's figure (Greenspan 2002).

Internet Usage and Monitoring

Adkins (2002) discusses the questions that employers often ask: How do you know when an employee uses the Internet, she/he uses it for business or pleasure? Is the employee using the company's email service for personal use, such as emailing family and relatives, or self-promoting their own sideline business? While acknowledging the productivity-related issues, Adkins points out that investing in sophisticated Internet monitoring and surveillance applications may only add to the cost without giving the organization the control over employees' online activities that it expects to achieve. He suggests the use of a written Internet Usage Policy as the first line of defense. Auditing or monitoring solutions should only be used in the event that the impact on productivity becomes obvious.

A feature article in the Information Management Journal discusses a 2001 Electronic Policies and Practices (EPP) survey conducted by the American Management Association (AMA), U.S. News and World Report, and The ePolicy Institute. The EPP survey pointed out that employers have become increasingly aware of the risks associated with workplace computing. Nearly 62 percent of the employers surveyed monitor their employees' email and Internet activities. For 68 percent of those who monitor, the primary driver is concern about legal liabilities stemming from Internet misuse or abuse. The survey also revealed that nearly 84 percent notified employees of the company's legal right to monitor online activity, whether any actual monitoring was carried out or not (Anonymous 2002).

The employees' right to privacy is a persistent issue that keeps on cropping up. McEvoy (2002) points out that while the laws protecting both the employers and employees is still in its infancy, the employee who uses the organization's email and Internet facilities for personal purposes does so at his or her peril.

A more recent survey (Hoffman et al. 2003) conducted by the Center for Business Ethics at Bentley College showed that 9 out of 10 companies monitoring their employees' use of the Internet and email. The survey also found that these companies monitored the employees' online activities constantly, not just when circumstances dictate the need for monitoring.

The primary question that this study hopes to answer is: Does the fact that a respondent knows that his/her Internet access is monitored have a positive effect on his/her attitude and perception of Internet access rights, online behavior and Internet usage? Stated formally, my first hypothesis is: *Knowing that one's Internet access is being monitored has a deterrent effect—employees behave better and will not abuse access rights*. Internet activities and usage frequency of both groups of respondents will be compared to determine whether there are any differences in online behavior and Internet usage between the Monitored and Unmonitored groups of respondents.

The employers' right to protect its

property as well as its right to protect itself from liabilities stemming from misuse or abuse of Internet facilities are the main arguments used to justify email and Internet monitoring in the workplace (Tidd 2002). As pointed out by Adkins (2002) and Tidd (2002), email and Internet usage policies provide protection for organizations while providing notice to employees of acceptable and appropriate online usage and behavior. How an IUP is crafted, deployed and communicated to the organization is critical to its successful implementation.

IUP Implementation

Martin (1999) discussed the basic challenges that managers need to address as they formulate an effective usage policy. How to control and limit personal use Internet facilities during working hours is one of the thorniest of management issues. The challenge is at once commercial and constitutional: How much control can companies effectively exert? Can it be done without rules stifling ease of communication? And how far do employees' individual rights of privacy and free speech extend in corporate cyberspace?

An organization's usage policy depends on the nature of the organization and its corporate culture. What may work with one organization may not necessarily work with another. While templates are available to help organizations rapidly develop IUPs that are legally sound, an IUP stands a much better chance of being successfully adopted if it is developed after consultations between management, workers, in-house computer experts and legal experts (Martin 1999). Making an effort to help employees appreciate the economic, legal and ethical reasons for the adoption of an IUP will certainly make compliance easier.

Cappel's study (2002) demonstrated that employees' acceptance of email monitoring is significantly greater when the policy has been communicated to employees. Providing notification of monitoring activities will help employers establish clear employee expectations as to levels of privacy when they use the Internet facilities in the workplace. This will also communicate to the employees that there is no attempt to surreptitiously spy on employee online activities.

However, despite efforts to develop and implement fair usage policies, Internet misuse and abuse continues to be a problem in the workplace. A survey of 224 organizations on issues related to Internet abuse (Greenfield and Davis 2002) showed that nearly 83 percent had usage policies detailing appropriate and inappropriate use of the Internet. The study revealed that despite usage policies, more than 60 percent had to discipline and 30 percent had to terminate employees for inappropriate use of the Internet. Equally disturbing was the fact that nearly 50 percent of the companies were not concerned about the severity of the problem or had done very little to enforce their usage policies.

The second question this study hopes to answer is: Does an employee's expectation of the IUP implementation match the reality of the actual implementation of an IUP? Stated formally, my hypothesis is: *An employee whose organization already enforces an IUP will have a more positive attitude towards the sustained implementation and evenhandedness of enforcement of an IUP than an employee with no experience complying with the provisions of an IUP.* The responses of both groups of respondents to questionnaire items dealing with IUP implementation will be compared to determine whether there are any differences between the expectations of the Without IUP group and the reality experienced by the With IUP group of respondents.

Methodology

The banking and finance sector was chosen as the initial target of this survey of Internet access practices and Internet usage policies mainly because of this sector's heavy dependence on Information Technology and the Internet in the conduct of business. This survey of selected Philippine banks and financial institutions was conducted from January to February 2003. The institutions were identified and selected through the help of the Bankers Institute of the Philippines, Inc. (BAIPhil). The key criterion for the selection of the banks and financial institutions to be surveyed was the availability of organization-wide Internet access facilities in the institutions' premises.

An original questionnaire was created for this study (see Appendix A). Copies of this self-administered questionnaire were delivered to the Human Resource Department (HRD) of each of the selected institutions. Since not all departments in the selected institutions were given access to the Internet, the HRD heads distributed the self-administered questionnaires to employees in departments/units that had all-day access to the Internet access facilities of the organization. Of the 200 questionnaires sent out, a total of 182 were completed and returned by the respondents, yielding a total response rate of 91 percent.

Among the Philippine banks and financial institutions surveyed were:

- Metropolitan Bank and Trust Company
- Equitable-PCI
- International Exchange Bank (I-Bank)
- Citibank
- China Bank
- Philippine Savings Bank
- Philippine Bank of Communication
- Allied Bank
- Representatives of member banks of the MegaLink consortium

The research instrument was designed to elicit the following information from the respondents:

- Their perception of the rights of the organization with regard to Internet resources and facilities at the workplace.
- Their perception of the rights of the individual with regard to Internet access at the workplace.
- The activities they engage in using the Internet access facilities during a typical workday.
- Their awareness of the organizations' Internet monitoring activities
- The nature, type, and frequency of usage of Internet facilities in the workplace
- Their perception of appropriate use of Internet facilities in the workplace.
- The availability or use of an Internet Usage Policy in the organization.
- Their perception of the consistency and evenhandedness of IUP implementation in their organizations

Respondent Profile

The 182 respondents belong to the banking and financial services sector with approximately 72 percent working with institutions that have been in business for over 25 years. About 65 percent of the respondents indicated that there were 10,000 or fewer employees in their organization. Over 54 percent of the respondents are between the ages of 25 to 39 while 35 percent are between 40 to 65 years of age. Nearly 60 percent of the respondents were female. Fewer than 65 percent of the respondents supervise employees.

Results and Discussion

Internet Access Rights

Appropriate use of internet facilities in the workplace (see Table 1)

Only nine out of the 182 respondents (4.95 percent) admitted to using their organization's Internet facilities for personal activities more than they should. Interestingly, nineteen respondents (10.44 percent) chose to remain neutral on the issue while 6.59 percent did not respond at all. This later finding gives rise to speculations that more respondents would actually admit to over-using the Internet facilities at work for non-work-related activities were it not for the possible negative repercussions of such an admission.

Monitoring of online activities at work (See Table 2)

Half of the respondents knew that their Internet activities were being monitored while 20.88 percent of the respondents indicated that their Internet access was not monitored. A surprising 27.47 percent of the respondents did not know if their online activities were being monitored.

The 92 respondents whose Internet access in the workplace is monitored were assigned to the Monitored group while the remaining 90 respondents were assigned to the Unmonitored group. The principal reason for dividing the sample into these two groups is to determine if the attitudes and behavior of respondents who know that their organizations monitor employee usage of Internet facilities will be different from those whose Internet access is not monitored. The rest of the discussion on Internet access issues will be based on the responses of these two groups.

Monitoring as a violation of privacy (see Table 3)

The contrast in the two groups' per-

Table 1. **Respondent Uses Internet Facilities for Personal Activities more than He/She Should**

	Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral	NR
I use the Internet for personal, non-work-related activities more than I should	53 29.12%	89 48.90%	8 4.40%	1 .55%	19 10.44%	12 6.59%

Table 2. **Respondent's Internet access is Monitored**

	Yes	No	Do Not Know	NR
My Internet access at work is monitored	92 50.55%	38 20.88%	50 27.47%	2 1.10%

Table 3. **Internet Access at Work: Comparison between Monitored Group and Unmonitored Group**

		Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral	NR
Monitoring Internet access at work violates my right to privacy	Monitored	10 10.87%	48 52.17%	7 7.61%	4 4.35%	22 23.91%	1 1.09%
	Unmonitored	5 5.56%	26 28.89%	27 30.00%	5 5.56%	23 25.56%	4 4.44%
I would not abuse Internet access at work even if it were not monitored	Mentioned	0 .00%	1 1.09%	49 53.26%	32 34.78%	9 9.78%	1 1.09%
	Unmonitored	0 .00%	0 .00%	43 47.78%	34 37.78%	6 6.67%	7 7.78%
I can be held liable for any illegal online activity I engage in while using the Internet access facilities at work	Monitored	1 1.09%	3 3.26%	59 64.13%	25 27.17%	3 3.26%	1 1.09%
	Unmonitored	1 1.11%	3 3.33%	56 62.22%	20 22.22%	4 4.44%	6 6.67%
My organization has the right to monitor my Internet access at work	Monitored	2 2.17%	4 4.35%	54 58.70%	24 26.09%	7 7.61%	1 1.09%
	Unmonitored	3 3.33%	13 14.44%	28 31.11%	10 11.11%	29 32.22%	7 7.78%
My organization can be held liable for any illegal online activity I engage in while using the Internet facilities at work	Monitored	7 7.61%	18 19.57%	42 45.65%	14 15.22%	10 10.87%	1 1.09%
	Unmentioned	1 1.11%	10 11.11%	42 46.67%	13 14.44%	16 17.78%	8 8.89%
My organization owns email and any document I send, receive, download or access using the Internet facilities at work	Monitored	2 2.17%	21 22.83%	41 44.57%	11 11.96%	15 16.30%	2 2.17%
	Unmonitored	5 5.56%	19 21.11%	33 36.67%	9 10.00%	19 21.11%	5 5.56%

Continued from Table 3

		Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral	NR
My organization has the right to read my incoming and outgoing email if it deems it necessary.	Monitored	5 5.43%	23 25.00%	41 44.57%	10 10.87%	12 13.04%	1 1.09%
	Unmonitored	13 14.44%	24 26.67%	29 32.22%	6 6.67%	13 14.44%	5 5.56%
My organization has the right to block access to sites on the World Wide Web	Monitored	1 1.09%	5 5.43%	60 65.22%	13 14.13%	11 11.96%	2 2.17%
	Unmonitored	1 1.11%	7 7.78%	54 60.00%	7 7.78%	14 15.56%	7 7.78%
My organization has the right to determine who is given Internet access at work	Monitored	0 .00%	2 2.17%	65 70.65%	20 21.74%	4 4.35%	1 1.09%
	Unmonitored	0 .00%	2 2.22%	57 63.33%	23 25.56%	2 2.22%	6 6.67%

ceptions about monitoring as a violation of privacy seems to imply that awareness of Internet monitoring in organizations that impose these controls may play a role in allaying fears related to the loss of privacy.

About 63 percent of the respondents in the Monitored group did not think that Internet monitoring was a violation of privacy while only 34.45 percent in the Unmonitored group thought likewise. There were far fewer respondents in the Monitored group who felt monitoring violated their privacy as compared with the Unmonitored group (11.96 percent versus 35.56 percent).

The respondents in the Monitored and Unmonitored groups who opted to remain neutral is rather large at 23.91 percent and 25.56 percent, respectively. The reason or reasons behind the lack of a definite stand on this sensitive issue may have its roots in the culture or in the norms of behavior expected of the workforce studied.

Organization's right to monitor online activities (see Table 3)

The difference between the groups' responses is rather stark. While 84.79 percent of the Monitored group acknowledged their organizations' right to monitor online activities, only 42.22 percent of the Unmonitored group did. On the other hand, the percentage of respondents giving a neutral response is far greater in the Unmonitored group (32.22 percent) than in the Monitored group (7.61 percent).

Organization's liability for employees' illegal online activities (see Table 3)

The majority of the respondents in

both groups agree that the organization can be held liable for any illegal activities employees engage in using the Internet facilities at work. Surprisingly, the percentage of respondents in the Monitored group who disagreed is high at 27.18 percent when compared with the Unmonitored group's 12.22 percent. In contrast, there were more respondents in the Unmonitored group who gave a neutral response (17.78 percent) than in the Monitored group (10.87 percent). This finding seems to indicate a lack of appreciation for the legal, reputational, and financial implications to the organization of employees' illegal online activities. The results also highlight the need to clearly define the boundaries of acceptable online behavior.

Organization's ownership of email and downloaded files (see Table 3)

At first glance, it may seem that a majority of respondents in both groups recognize the organization's right of ownership over email and any material downloaded using the Internet facilities at work. However, the percentage of respondents in both groups who did not agree is disturbingly large at 25 percent and 26.67 percent, respectively. Likewise, the percentage of respondents in both groups who gave a neutral response was also rather high at 16.30 percent and 21.11 percent, respectively.

These findings raise concerns that employees may not fully understand the basic premise underlying management's investment in Internet facilities – that these facilities are provided primarily for the conduct of business and as such, any material or communication passing through these facilities are the property of the organization.

Organization's right to read employees' email (see Table 3)

Only 55.44 percent of the Monitored group acknowledged the right of the organization to read employee email compared to 38.89 percent in the Unmonitored group. The percentage of respondents in the Monitored and Unmonitored groups disagreeing with the statement is at 30.43 percent and 41.11 percent, respectively. The respondents in both groups giving a neutral response is about equal at 13.04 percent and 14.44 percent, respectively.

The results point out a disturbing fact: Privacy and ownership of email remains a thorny issue even in organizations that have been openly monitoring Internet. It highlights the lack of understanding about the organization's rights in relation to the provision of Internet access. It also highlights the need to manage user expectations about levels of privacy on a corporate network. Finally, the results underscore the importance of clearly defining the rights and obligations of both the organization and the users of the Internet facilities at work.

Other findings pertaining to Internet Access Rights issues (see Table 3)

While majority of the respondents in both groups acknowledged their organizations' right to limit the websites employees could access from the workplace, the number of respondents in the Monitored and the Unmonitored groups who opted to remain neutral constitutes 11.96 percent and 15.56 percent, respectively. These numbers are sufficiently large to merit closer examination, particularly by administrators who must implement the organizations' Internet monitoring and control policies.

The responses of both groups reflected the fact that the respondents would not abuse the right to use Internet facilities at work even if their organizations did not monitor their online activities.

Respondents in both groups also understood that they were liable for the consequences of any illegal activity they engage in using the organization's Internet facilities. The results indicate that the respondents understood the responsibilities and obligations associated with the grant of Internet access at work.

Both groups of respondents were nearly unanimous in acknowledging the organization's right to select who among its employees would be given access to its Internet facilities. This finding is specially important in the Philippine context where access to the organization's Internet facilities is not a right that employees can take for granted but is a privilege that management extends to certain individuals only. In most cases, the need to be selective is a direct result of limited bandwidth and computer resources.

Internet Usage in the Workplace

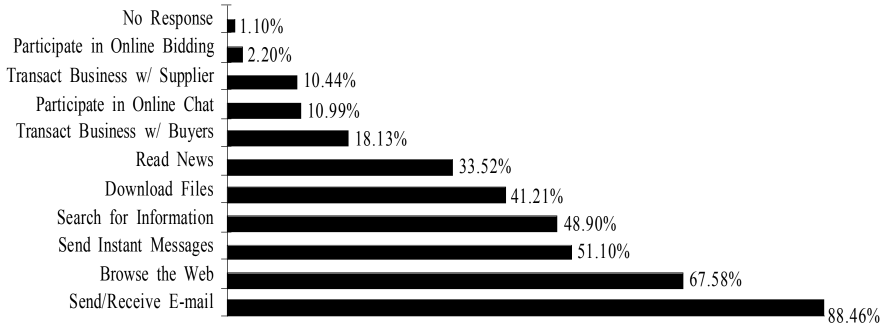
Attitude towards personal use of internet access facilities at work (see Table 4)

While 46.16 percent of the respondents believed it was alright to use these facilities for non-work-related activities, reflecting a basic understanding of the purpose for which their organizations provided Internet facilities at work, nearly 20

Table 4. **Nonwork-related Use of the Internet Facilities in the Workplace Is Alright**

	Strongly Disagree	**Disagree**	**Agree**	**Strongly Agree**	**Neutral**	**NR**
I believe it is alright to use the Internet for personal, non-work related activities	8	28	80	4	55	7
	4.40%	15.38%	43.96%	2.20%	30.22%	3.85%

Figure 1. **Types of Online Activities Using Internet Facilities in the Workplace**



	Send/Receive E-mail	**Online Bidding**	**Browse Web**	**Transact Business w/ Supplier**	**Instant Messages**	**Transact Business w/ Buyers**	**Chat**	**Search for Information**	**Download Files**	**Read News**	**NR**
My internet access at work allows me to engage in the following activities:	161	4	123	19	93	33	20	89	75	61	2
	88.46%	2.20%	67.58%	10.44%	51.10%	18.13%	10.99%	48.90%	41.21%	30.52%	1.10%

percent disagreed with the statement. These findings, coupled with a neutral response rate of 30.22 percent, also reflect the need for an unambiguous statement about acceptable personal use of Internet facilities at work.

Respondents' online activities using internet facilities at work (See Figure 1)

The top five activities of the respondents are sending/receiving email, browsing, sending instant messages, searching for information and downloading files. Interestingly, a third of the respondents read the news. About 11 percent of the respondents were candidly acknowledged engaging in online chats while at work.

Usage of internet facilities for work-related activities (see Table 5)

Philippine banks and financial institutions observe a 40-hour workweek. The results of the survey show that 52.20 percent of the 182 respondents use the Internet facilities in the workplace five hours or less a week for work-related activities. As part of their jobs, 20.88 percent of the respondents indicated that they spend six to ten hours online. Only 7.69 percent spent more than half of the 40-hour workweek online performing work-related activities. Interestingly, 9.89 percent of the respondents refused to indicate the amount of time they spent online.

Usage of internet facilities for non-work-related activities (see Table 5)

In comparison, 76.92 percent of the respondents admitted to using the Internet facilities in the workplace five hours or less a week for nonwork-related activities. The nature of the data being gathered and the conclusions that may be drawn about the productivity of the respondents may have a bearing on the fact that 13.74 percent of the respondents refused to reveal the actual number of hours they spent online for nonwork-related activities.

Send/receive nonwork-related email using internet facilities at work (see Table 6)

Eighty-six respondents (47.25 per-

Table 5. **Average Number of Hours per Week Spent Using the Internet Facilities in the Workplace**

	1 - 5 hours	**6 - 10 hours**	**11 - 15 hours**	**15 - 20 hours**	**> 20 hours**	**NR**
The average number of hours I spend per week using the Internet access facilities at work	95 52.20%	38 20.88%	8 4.40%	9 4.95%	14 7.69%	18 9.89%
The average number of hours I spend per week using the Internet access facilities at work for personal, non-work-related activities	140 76.92%	13 7.14%	3 1.65%	1 .55%	0 .00%	25 13.74%

cent) used the Internet facilities in the workplace to send or receive personal, nonwork-related email five times or less during the preceding month. Exactly 14.29 percent of the respondents never sent or received personal email at work during the preceding month while 14.84 percent sent / received personal email over 15 times during the same period. Interestingly, 6.04 percent of the respondents refused to indicate how often they used the Internet facilities at work for personal email.

Use internet facilities at work for nonwork-related activities (see Table 6)

Forty-five percent of the respondents used the Internet facilities at work for nonwork-related activities five times or less during the preceding month while 32.42 percent never used the Internet facilities for non-work-related activities. Nearly 11% of the respondents used these facilities 10 times or less while 3.30 percent used the Internet facilities for non-work-related activities beyond 15 times during the same period.

Purchase a Nonwork-related Item Using Internet Facilities at Work (See Table 6)

Nearly 85 percent or 154 out of 182 respondents never made an online purchase. Of those who did, only 6.04 percent purchased a nonwork-related item online more than five times in the preceding month. Eleven respondents (6.04 percent) refused to reveal how often they used the Internet facilities at work to make personal purchases online.

Download nonwork-related files using Internet facilities at work (See Table 6)

During the preceding month, 15.93 percent of the respondents downloaded nonwork-related files five times or less using the Internet facilities at work. Majority of the respondents (74.18 percent) never downloaded nonwork-related files during the same period. Only one respondent

Table 6. **Frequency of Use of Internet Access Facilities in the Workplace During Preceding Month**

	Never	1 - 5 times	6 - 10 times	11 - 15 times	Over 15 times	NR
In the past month, I sent and / or received non-work related email while at work	26 14.29%	86 47.25%	24 13.19%	8 4.40%	27 14.84%	11 6.04%
In the past month, I have accessed the Internet for non-work-related activities while at work	59 32.42%	82 45.05%	20 10.99%	5 2.75%	6 3.30%	10 5.49%
In the past month, I have purchased a non-work related item via the Internet while at work	154 84.62%	6 3.30%	11 6.04%	0 .00%	0 .00%	11 6.04%
In the past month, I have downloaded files (programs, music, etc.) for personal use while at work	135 74.18%	29 15.93%	4 2.20%	1 .55%	1 .55%	12 6.59%

admitted to downloading personal files over 15 times in the past month. Twelve respondents (6.59 percent) did not reveal the number of times they downloaded nonwork-related files using Internet facilities in the workplace.

IUP Implementation Concerns

Respondent's organization has an Internet Usage policy (see Table 7)

While 38.46 percent of the respondents indicated that their organization had an Internet Usage Policy (IUP), 21.98 percent indicated that their organization did not have one. The percentage of respondents who they did not know if the organization had an IUP was a disturbing 32.97 percent.

The respondents who indicated that their organization had an IUP were assigned to the *With IUP* group while the rest were assigned to the *Without IUP* group. One of the reasons for implementing an IUP is to establish the boundaries of acceptable online behavior and appropriate usage of the organization's Internet access facilities. Grouping the respondents in this manner will be used to validate if the presence of an IUP does indeed prevent the abuse of the Internet facilities in the workplace. Another purpose is to gauge the respondents' attitude toward IUPs as a control mechanism. Further discussion of IUP implementation issues will be based on these groups' responses.

Respondent will comply with IUP if made a condition of employment (see Table 8)

It appears that the respondents belonging to the With IUP group are unhappy with the notion that employment or continued employment in their respective organizations could be tied to compliance with the IUP provisions. Exactly 50 percent of the respondents in this group indicated outright that they would not abide by the IUP provisions under those conditions while 41.43 percent indicated they would.

On the other hand, the results obtained from the Without IUP group reflected a more positive outlook where 87.50 percent indicated that, even under those conditions, they would comply with the IUP provisions should their organization impose one. Having had no experience in dealing with the restrictions on Internet usage that an IUP may impose, this group may be expecting an ideal setup similar to their current one but with a few minor rules for them to observe. While no respondents indicated they would not abide by the IUP provisions, 10.71 percent did not respond at all.

Respondent will comply with IUP even if not a condition of employment (see Table 8)

In contrast with the preceding set of

Table 7. **Organization has an Internet Usage Policy**

	Yes	No	Do not Know	NR
My organization has an Internet Usage Policy (IUP)	70 38.46%	40 21.98%	60 32.97%	12 6.59%

results, the responses of the group working for organizations with IUPs were far more positive without the condition of employment or continued employment tied to the observance of IUP provisions. A total of 85.71 percent indicated that they would abide by the IUP terms.

The responses of the group working for organizations without IUPs are equally interesting. Without the employment (or continued employment) condition, only 77.68 percent of the respondents indicated that they would abide by the IUP provisions should the organization impose one in the future. Interestingly, 12.50 percent of the group did not respond at all.

Strict enforcement of IUP across all levels of the organization (See Table 9)

The group with IUPs had 74.29 percent of respondents indicating that the IUP provisions are strictly enforced across all levels of the organization. Another 15.71 percent didn't know if the IUP was strictly implemented across all levels.

While 86.61 percent of the group without IUPs believed that the provisions of any future IUP would be strictly enforced, 9.82 percent of this group gave no response at all.

Sustained Implementation of IUP provisions (See Table 9)

Less than 69 percent of the respondents from organizations with IUPs agreed that their organizations made a sustained effort to ensure that employees complied with IUP provisions. Nearly 9 percent thought otherwise while an unexpectedly large number of respondents (22.86 percent) did not know if the organization did.

In contrast, 83.04 percent of the group without IUPs conveyed the belief that their organizations would make a sustained effort to ensure that employees comply with IUP provisions. Curiously, 11.61 percent of this group gave no response at all.

IUP used to discipline violators regardless of rank or position (See Table 9)

Table 8. **Compliance with IUP Provisions as a Condition of Employment: Comparison of responses**

		Yes	No	Do not Know	NR
I would abide by the terms of the Internet Usage Policy if it were made a condition of my employment (or continued employment)	With IUP	29 41.43%	35 50.00%	6 8.57%	0 .00%
	Without IUP	98 87.50%	0 .00%	2 1.79%	12 10.71%
I would abide by the terms of the IUP even if it were NOT a condition of my employment (or continued employment)	With IUP	60 85.71%	2 2.86%	5 7.41%	3 4.29%
	Without IUP	87 77.68%	6 5.36%	5 4.46%	14 12.50%

The data gathered from the respondents belonging to organizations with IUPs is rather surprising. Only 54.29 percent agreed that the organization disciplined users for IUP violations regardless of rank or position while 37.14 percent indicated they did not know if the organizations did. In comparison, 82.14 percent of respondents from organizations without IUPs expect violators of IUP provisions to be disciplined regardless of rank or position. A surprising 10.71 percent of this group did not respond.

IUP will eliminate or reduce personal use of Internet facilities (see Table 10)

Majority of the respondents in both groups agreed that the use of IUPs is an effective way to eliminate or at least reduce non-work-related use of Internet facilities in the workplace. An unexpected finding is that 11.43 percent of the group with IUPs and 17.86 percent of the group without IUPs opted to remain neutral. Another 11.61 percent of the latter group did not respond

Table 9. **Internet Usage Policy Implementation Concerns: Comparison of Responses**

		Yes	No	Do not Know	NR
Organization's Internet Use Policy is (*should be*) enforced across all levels of the organization	With IUP	52 74.29%	5 7.14%	11 15.71%	2 2.86%
	Without IUP	97 86.61%	1 .89%	3 2.68%	11 9.82%
Organization makes (*should make*) a sustained effort to ensure that all employees abide by the terms of the policy	With IUP	48 68.57%	6 8.57%	16 22.86%	0 .00%
	Without IUP	93 83.04%	2 1.79%	4 3.57%	13 11.61%
Organization disciplines (*should discipline*) any user who does not abide by the terms of the policy, regardless of rank or position	With IUP	38 54.29%	6 8.57%	26 37.14%	0 .00%
	Without IUP	92 82.14%	6 5.36%	2 1.79%	12 10.71%

Table 10. **IUP Is an Effective Way to Eliminate/Reduce Personal Use of Internet Facilities at Work**

		Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral	NR
Overall, I believe that an Internet Usage Policy is an effective way to eliminate or at least reduce personal Internet and e-mail usage at work	With IUP	1 1.43%	4 5.71%	39 55.71%	14 20.00%	8 11.43%	4 5.71%
	Without IUP	5 4.46%	5 4.46%	50 44.64%	19 16.96%	20 17.86%	13 11.61%

at all.

Statistical Analysis

Analysis of Variance

1) *H_o: Knowing that one's Internet access is being monitored has deterrent effect – employees behave better and will not abuse access rights*
   H_a: Otherwise

--> *H_o:* Internet usage for personal, non-work related activities of employee who *knows* that his/her Internet access is monitored < Internet usage of a respondent who *does not know* that his/her Internet access is monitored.The results are as follows.

2) *H_o: An employee whose organization already enforces an IUP will have a more positive attitude towards the sustained implementation and evenhand-*

Descriptives

							95% Confidence Interval for Mean			
			N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Min	Max
hrwk_40	Yes		86	1.9419	1.38356	.14919	1.6452	2.2385	1.00	5.00
	No		37	1.9730	1.36395	.22423	1.5182	2.4277	1.00	5.00
	Do not know		45	1.7333	1.11600	.16636	1.3981	2.0686	1.00	5.00
	Total		168	1.8929	1.30882	.10098	1.6935	2.0922	1.00	5.00
	Model	Fixed Effects			1.31306	.10131	1.6928	2.0929		
		Random Effects				.10131(a)	1.4570(a)	2.3287(a)		
hrper_41	Yes		80	1.1250	.51250	.05730	1.0109	1.2391	1.00	5.00
	No		33	1.1212	.33143	.05770	1.0037	1.2387	1.00	2.00
	Do not know		41	1.1220	.50966	.07960	.9611	1.2828	1.00	4.00
	Total		154	1.1234	.47593	.03835	1.0476	1.1991	1.00	5.00
	Model	Fixed Effects			.47907	.03860	1.0471	1.1997		
		Random Effects				.03860(a)	.9573(a)	1.2895(a)		
nwrel_44	Yes		87	2.5632	1.18813	.12738	2.3100	2.8164	1.00	5.00
	No		38	2.6053	1.42449	.23108	2.1370	3.0735	1.00	5.00
	Do not know		47	2.5106	1.31665	.19205	2.1241	2.8972	1.00	5.00
	Total		172	2.5581	1.27141	.09694	2.3668	2.7495	1.00	5.00
	Model	Fixed Effects			1.27847	.09748	2.3657	2.7506		
		Random Effects				.09748(a)	2.1387(a)	2.9776(a)		
accnw_45	Yes		87	2.0000	.97647	.10469	1.7919	2.2081	1.00	5.00
	No		37	2.1081	1.10010	.18085	1.7413	2.4749	1.00	5.00
	Do not know		46	1.9565	.75884	.11189	1.7312	2.1819	1.00	4.00
	Total		170	2.0118	.94830	.07273	1.8682	2.1553	1.00	5.00
	Model	Fixed Effects			.95240	.07305	1.8676	2.1560		
		Random Effects				.07305(a)	1.6975(a)	2.3261(a)		

Continued from Descriptives

							95% Confidence Interval for Mean			
			N	**Mean**	**Std. Deviation**	**Std. Error**	**Lower Bound**	**Upper Bound**	**Min**	**Max**
purnw_46	Yes		87	1.0345	.18352	.01968	.9954	1.0736	1.00	2.00
	No		38	1.0526	.32444	.05263	.9460	1.1593	1.00	3.00
Do not know			46	1.0217	.14744	.02174	.9780	1.0655	1.00	2.00
	Total		171	1.0351	.21406	.01637	1.0028	1.0674	1.00	3.00
	Model	Fixed Effects			.21505	.01645	1.0026	1.0676		
		Random Effects				.01645(a)	.9643(a)	1.1058(a)		
dwnld_47	Yes		87	1.2299	.56447	.06052	1.1096	1.3502	1.00	5.00
	No		38	1.2895	.56511	.09167	1.1037	1.4752	1.00	3.00
	Do not know		45	1.2000	.45726	.06816	1.0626	1.3374	1.00	3.00
	Total		170	1.2353	.53619	.04112	1.1541	1.3165	1.00	5.00
	Model	Fixed Effects			.53845	.04130	1.1538	1.3168		
		Random Effects				.04130(a)	1.0576(a)	1.4130(a)		

Test for Homogeneity of Variances
(H_o: equal variances for different groups, $\alpha = .05$)

	Levene Statistic	**df1**	**df2**	**Sig.**
hrwk_40	.975	2	165	.379
hrper_41	.015	2	151	.985
nwrel_44	1.564	2	169	.212
accnw_45	.615	2	167	.542
purnw_46	.916	2	168	.402
dwnld_47	.922	2	167	.400

With alpha > .05, we will accept the null hypothesis and conclude that the variances of the groups are equal.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
hrwk_40	Between Groups	1.589	2	.795	.461	.632
	Within Groups	284.482	165	1.724		
	Total	286.071	167			
hrper_41	Between Groups	.000	2	.000	.001	.999
	Within Groups	34.655	151	.230		
	Total	34.656	153			
nwrel_44	Between Groups	.193	2	.096	.059	.943
	Within Groups	276.226	169	1.634		
	Total	276.419	171			
accnw_45	Between Groups	.496	2	.248	.273	.761
	Within Groups	151.481	167	.907		
	Total	151.976	169			
purnw_46	Between Groups	.020	2	.010	.215	.806
	Within Groups	7.770	168	.046		
	Total	7.789	170			
dwnld_47	Between Groups	.170	2	.085	.293	.746
	Within Groups	48.418	167	.290		
	Total	48.588	169			

With alpha > .05, we will accept the null hypothesis and conclude that knowing one's internet access is being monitored has deterrent effect —employees bahave better and not abuse access rights.

edness of enforcement of an IUP than an employee with no experience complying with the provisions of an IUP.

H_a: Otherwise

-->H_o: Attitude of employee *who knows* that an IUP is enforced in their organization > Attitude of employee *who does not know* that an IUP is enforced in their organization.

Descriptives

							95% Confidence Interval for Mean			
			N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Min	Max
enfor_52	Yes		73	1.3973	.77710	.09095	1.2159	1.5786	1.00	3.00
	No		38	1.0263	.16222	.02632	.9730	1.0796	1.00	2.00
	Do not know		61	1.1475	.51108	.06544	1.0166	1.2784	1.00	3.00
	Total		172	1.2267	.61253	.04670	1.1346	1.3189	1.00	3.00
	Model	Fixed Effects			.59647	.04548	1.1370	1.3165		
		Random Effects					.11260	.7422	1.7112	
abide_53	Yes		74	1.5541	.84630	.09838	1.3580	1.7501	1.00	3.00
	No		37	1.0000	.00000	.00000	1.0000	1.0000	1.00	1.00
	Do not know		61	1.1148	.41224	.05278	1.0092	1.2203	1.00	3.00
	Total		172	1.2791	.65160	.04968	1.1810	1.3771	1.00	3.00
	Model	Fixed Effects			.60804	.04636	1.1875	1.3706		
		Random Effects					.18018	.5038	2.0543	
disc_54	Yes		74	1.8514	.94626	.11000	1.6321	2.0706	1.00	3.00
	No		38	1.0789	.27328	.04433	.9891	1.1688	1.00	2.00
	Do not know		61	1.1639	.52219	.06686	1.0302	1.2977	1.00	3.00
	Total		173	1.4393	.78730	.05986	1.3212	1.5575	1.00	3.00
	Model	Fixed Effects			.70498	.05360	1.3335	1.5451		
		Random Effects					.26506	.2989	2.5798	

Test of Homogeneity of Variances (Ho: equal variances for different groups, $\alpha = .05$)

	Levene Statistic	df1	df2	Sig.
enfor_52	27.813	2	169	.000
abide_53	79.020	2	169	.000
disc_54	85.802	2	170	.000

With alpha > .05, we will accept the null hypothesis and conclude that the variance of the groups are not equal.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
enfor_52	Between Groups	4.032	2	2.016	5.666	.004
	Within Groups	60.125	169	.356		
	Total	64.157	171			
abide_53	Between Groups	10.124	2	5.062	13.692	.000
	Within Groups	62.481	169	.370		
	Total	72.605	171			
disc_54	Between Groups	22.124	2	11.062	22.258	.000
	Within Groups	84.489	170	.497		
	Total	106.613	172			

With alpha > .05, we will reject the null hypothesis and conclude that an employee with no experience complying with the provisions of an IUP will have a more positive attitude towards the sustained implementation and evenhandedness of enforcement of an IUP than an employee whose organization already enforces an IUP.

Reliability Analysis

Item Means	Mean	Minimum	Maximum	Range	Max/Min	Variance
Part 1	2.6534	1.0909	4.3818	3.2909	4.0167	1.3032
Part 2	2.0455	1.0182	4.1818	3.1636	4.1071	1.0369
Scale	2.3544	1.0182	4.3818	3.3636	4.3036	1.2467

Inter-item Correlations	Mean	Minimum	Maximum	Range	Max/Min	Variance
Part 1	.0510	-.6177	.9918	1.6094	-1.6057	.0429
Part 2	.0381	-.4076	.8792	1.2868	-2.1568	.0356
Scale	.0153	-.7552	1.0000	1.7552	-1.3241	.0338

Analysis of Variance

Source of Variation	Sum of Sq.	DF	Mean Square	F	Prob.
Between People	67.5243	54	1.2504		
Within People	6066.0984	3300	1.8382		
Between Measures	4114.0590	60	68.5677	113.8088	.0000
Residual	1952.0393	3240	.6025		
Total	6133.6227	3354	1.8287		
Grand Mean	2.3544				

Reliability Coefficients 61 items

```
Correlation between forms = .0419        Equal-length Spearman-Brown = .0805
Guttman Split-half = .0805               Unequal-length Spearman-Brown = .0805
Alpha for part 1 = .5684                 Alpha for part 2 = .4437
31 items in part 1                       30 items in part 2
```

The results tell us that the questionnaire is highly reliable with alpha equal to .5684 and .4427.

Conclusions and Recommendations

On the Appropriate Use of Internet facilities in the Workplace

An IUP should reiterate the business reasons why Internet facilities are made available in the workplace. Reminding the employees of these reasons through an IUP is a good way to help them understand the need to reduce or eliminate personal online activities during work hours.

While fear of possible censure or curtailment of access rights is the probable reason for the lack of response to this survey's personal usage questions, a clear and unambiguous Internet Usage Policy statement will go a long way towards educating the organization's Internet users on the rights and obligations of all parties.

There is a need to clearly define the expected employee behavior and responsibilities associated with the use of Internet access facilities at work. Equally important is a specific and unambiguous statement of sanctions or penalties for abuse of these facilities. An IUP should clearly state the type of online activities allowed during work hours as well as the purpose and frequency of these activities. Should any personal use of the Internet access facilities be allowed at work, the IUP should clearly state the parameters under which these are allowed. Clearly stating the time during the workday and the frequency that employees can use the Internet facilities for personal activities will go a long way towards reducing non-work-related use of the Internet.

On the Rights and Liabilities of the Organization

The findings on the issues of monitoring, privacy and ownership of correspondence should serve as wake-up call for administrators and managers. The numbers reflect the lack of understanding of the rights of the organization well as the limitations on the privacy and usage that individuals can expect when using the Internet facilities in the workplace. While access monitoring and ownership of email are management prerogatives, it would not hurt for the reasons behind such policies to be understood by all. Holding discussions on these issues will foster better understanding of the concerns of both management and staff.

There is a need to educate users about the process of monitoring Internet access. A clear statement about the nature and purpose of Internet monitoring will go a long way towards maintaining the trust of employees. Openly communicating the reasons behind the need for controls on Internet access will encourage employees to cooperate and help the organization maintain the integrity of its data and systems.

Among the important points about monitoring that should be stated in an IUP are:

- the reasons why the organization monitors online activities,
- the extent of the monitoring (what, when and how online activities are monitored),
- who does the monitoring,
- what protection employees will have against harassment or misuse of the data gathered about one's online activities, and
- who will have access to the data about the employees' online habits.

The responses of both Monitored and Unmonitored groups illustrate a lack of understanding of the legal and reputational risks that employees' illegal online activities expose the organization to. The use of corporate Internet access facilities for illegal or harmful online activities like gambling, running online scams, spreading viruses, distributing spam, pornographic material, hate mail and the like exposes the organization to legal action by victims of such illegal online activities. At the same time, the risk to the organization's reputation brought on by the perception that the organization (and by extension, their employees) engages in illegal activities can have major adverse economic implications to everyone in the organization.

An organization's IUP should contain a clear statement about the extent of its liabilities in the event that employees engage in illegal online activities. The organization should discuss the economic repercussions and the damage to the organization's reputation that could happen through employees' illegal or improper online behavior. Actual cases should be cited to give employees concrete examples of what constitutes illegal online activities or improper online behavior. These case discussions should include a description of the economic cost to the organization and the extent of the damage to its reputation (if any occurred).

On Internet Usage

Administrators should recognize that the use of Internet facilities at work to send instant messages (IMs) eats up precious bandwidth and distract employees from their works. There are definite productivity related issues associated with the use of IM applications at work that should be further studied in future research.

The downloading of files by employees with access to the Internet present security-related issues. Administrators must realize that certain types of malicious code can be used by unscrupulous individuals to gain access to the organization's data and applications, resulting in damage to or loss of the organization's information resources with its obvious financial and operational repercussions. In the very least, the need to clear a network of any viruses has its attendant costs in terms of time, effort, and lost opportunities.

While reading news online is not really a time wasting activity, it may have major implications on the bandwidth available to other members of the organization who may have more important online activities to carry out. Clear policies on the appropriate use of Internet facilities may help ease the bandwidth problem, especially in organizations with limited I.T. resources.

The use of the term 'browsing' in the survey was deliberate. It is obviously not a business-related activity but is more of a personal online activity that carries connotations of a rather relaxed, non-urgent exploration for something interesting. The fact that 67.58 percent of the respondents browse the WWW at work suggests that the bandwidth problem may be eased by being selective about who is allowed to access the WWW during office hours. To forestall complaints about favoritism or bias when such a solution is implemented, some organizations have taken steps to identify off-peak hours where limited surfing or browsing is allowed.

While the data on work-related and nonwork-related use of Internet facilities elicited in this survey are interesting, the real challenge for managers is to identify the actual job-related uses for Internet access as well as to determine the true levels of Internet use in their respective areas. This will definitely have a positive effect on efforts to equitably allocate the available bandwidth and Internet facilities of the organization.

On Internet Usage Policy Implementation

A simple inspection of Table 9 shows that the respondents from the group without IUPs consistently had more positive expectations of the IUP implementation process compared with the group that already had IUPs in place.

Preparing the organization by disseminating information about the existence of the IUP, its provisions, the internal and external factors that make its adoption a necessity, the benefits to the organization, and the consequences of nonadoption is a necessary step towards the successful adoption and implementation of an IUP.

All employees must read the IUP and acknowledge having read it. This acknowledgement is essential to protect the organization from charges that it failed to inform the users of the Internet facilities of the IUP provisions and the penalties for any violation of those provisions.

Administrators and managers should be conscious about the possibility that employees can negatively perceive the IUP as a behavior control mechanism. The responses to two statements in the survey provide a study in contrast. The first statement, ‘I will abide by the terms of the IUP if it were made a condition of my employment (or continued employment),’ generated a surprising response from the respondents working in organizations that had already implemented IUPs. Half of the respondents in this group indicated they would not comply with the IUP provisions. In the second statement, ‘I will abide by the terms of the IUP if it were NOT a condition of my employment (or continued employment),’ only 2.86 percent of the respondents in the same group indicated they would not comply with the IUP provisions.

Further research could examine if there is a cultural basis for such a reaction. What the research suggests is that, for this particular sample, there is a negative reaction to the use of implied threats to employment (or continued employment) to ensure compliance with the IUP provisions.

If management is to be perceived as evenhanded in its implementation of the organization’s IUP, it has to take steps to communicate its efforts at strictly enforcing the IUP terms across the entire organization. A good way to do this is to issue periodic bulletins stating the levels of usage of the Internet facilities and the types of violations during a given period. While identifying the violators by name would probably be counter-productive, drawing up a profile of the violators, their rank and the penalties or sanctions for their violations will probably be enough to send the message that the organization is serious about the implementation of the IUP. Sending reminders about the IUP’s provisions at regular intervals via email will also reinforce the perception that the management is making a sustained effort to implement its IUP across all levels of the organization.

The Internet's impact on banking and financial service institutions is considerable. Whether these institutions are ready or not, the Internet is here and it is here to stay. The benefits the Internet provides is indisputable but organizations must recognize and deal with productivity-related issues and liabilities. Nolan (2003) suggests that both employers and employees can and should do their part in minimizing Internet abuse. Employees can do so by being conscious of the reason employers provide computers, systems, and Internet access in the workplace. Employers should resist the temptation to adopt draconian policies. Finally, management should make an effort to lay the groundwork for organizational acceptance of the Internet Usage Policy through open discussion of the issues and concerns of all stakeholders.

Limitations of the Study

First, the data used in this study was elicited using a self-administered questionnaire survey. Bias may have resulted from the institution and respondent selection process. The respondent selection within the target banks and financial institutions was not random in the sense that the HRD heads selected the departments to be surveyed and the respondents for the survey questionnaire.

Second, this study focused only on the Internet access issues and IUP implementation concerns of selected Philippine banks and financial institutions. No generalizations, therefore, can be made from the conclusions made in this study. A broader perspective and understanding of the issues relating to the use of Internet access facilities in the workplace could be had by running the survey across industries and sectors, and across cultural groups or nations.

Directions for Future Research

Future research should be directed at gaining data about the Internet access practices and usage in the workplace in other industries and sectors. It is likely that different industries and sectors will have different needs and will thus use their Internet facilities differently from the financial sector. The data gathered would greatly help managers and administrators develop policies that directly address the needs of their particular sector. Such Internet usage policies and implementation practices will serve to maximize their investment in the I.T. infrastructure needed to support the conduct of business online and will minimize conflict and misunderstanding relating to Internet access and privacy rights within the organization.

Another possible direction for future research is taking a closer look at some of the cultural and human behavior issues relating to Internet use in the workplace and IUP implementation. Issues like privacy, the concept of personal and institutional liability for online behavior, open communication relating to sanctions resulting from IUP infractions, perceptions of evenhanded implementation of IUP provisions are just some of the areas that need to be investigated further. How will employees of financial institutions in other Asian countries respond to the same questionnaire? How will employees in other industries in other Asian countries respond? Will there be a difference between the responses of non-Asians as compare with Asians?

More research also needs to be done in the IUP implementation area. Specific practices, the results of implementation as well as cases need to be documented and communicated to help other administrators.

Finally, research needs to be done in two major areas where the Internet is getting to be a critical and important factor in day-to-day operations. These are the use of the Internet within government as well as its use in the academe. Given the budgetary limitations in these sectors, finding out how the Internet access facilities are used is the key to developing usage policies that will reflect the different needs and conditions within these sectors.

References

Adkins, A. Z. 2002. Employee Use of the Internet. Retrieved February 07, 2003 from http://www.lawcommerce.com/t3/art_adkins_eeinternetuse.asp

Anonymous. 2002. Company Email: To Monitor or not to Monitor. *Information Management Journal* 36 (8): 8.

Cappel, J. J. 1995. A Study of Individuals' Ethical Beliefs and Perceptions of Electronic Mail Privacy. *Journal of Business Ethics* 14(10): 819-827.

Carliner, S. 1999. An Overview of On-Line Learning. Retrieved on May 29, 2002 from http://www.lakewoodconferences.com/wp/first.htm

Goss, E. 2001. The Internet's contribution to U.S. productivity growth. *Business Economics.* 36 (4): 32-42.

Greenfield, D. N., and R. A. Davis. 2002. Lost in Cyberspace: The Web @ Work. *CyberPsychology and Behavior* 5(4): 347- 353.

Greenspan, R. 2002. Internet Abuse Drains Time and Money. Retrieved February 06, 2003 from http://clickz.com/stats/markets/professional/article.php/5971_1551411

Hoffman, W. M., L. P. Hartman, and M. Rowe. You've Got Mail… and the Boss Knows: A Survey by the Center for Business Ethics of Companies' Email and Internet Monitoring. *Business and Society Review* 108(3): 285-307

Hyman, G. 2002. Web Addiction on the Rise. Retrieved January 30, 2003 from http://siliconvalley.internet.com/news/article.php/1450351

Litan, R. E., and A. M. Rivlin. 2001. Projecting the Economic Impact of the Internet. *American Economic Review* 91(2): 313-317.

Martin, J. 1999. Internet Policy: Employee Rights and Wrongs. *HR Focus* 76(3): 1-12

McEvoy, S. 2002. Email and Internet Monitoring and the Workplace: Do Employees have the Right to Privacy? *Communications and the Law* 24(2): 69.

Nolan, D. 2003. Privacy and Profitability in the Technological Workplace. *Journal of Labor Research* 24(2): 207.

Oliner, S. D., and D. E. Sichel. 2000. The Resurgence of Growth in the Late 1990s: Is

Information Technology the Story? *Journal of Economic Perspectives.* 14(4): 3-22.

Standler, R. B. 2002. Issues in Computer Acceptable Use Policy. Retrieved December 12, 2002 from http://www.rbs2.com/policy.htm

TechWeb.com. Accessed on March 20, 2004 from http://techweb.com/encyclopedia/

Tidd, R. R. 2002. Privacy Practices and Policies: Protection and Confidence in a Networked Environment. *Taxes* 80(4): 5-6.

Vault.com. 2000. Survey of Internet Use in the Workplace. Retrieved February 25, 2003 from http://www.vault.com/surveys/internetuse2000/index2000.jsp.

APPENDIX

Internet Usage Survey

The purpose of this survey is to evaluate how the Internet is used during work hours. The survey has 4 sections with a total of 62 questions, but only 46 of which you will need to answer. Check the tick box beside the most appropriate response to each question. Please do not leave any question unanswered. The approximate time to complete this survey is about 25 minutes or less. Thank you very much for your time and patience.

Section 1: Respondent's Profile

1. Please indicate which of the following best describes your employer's industry.
○ Consulting ○ Education ○ Finance/Banking ○ Government
○ Health Care ○ Insurance ○ Manufacturing ○ Transportation / Distribution
○ Technology ○ Service ○ Retail ○ Other (Pls. Specify) _______________

2. How long has the organization you work for been in business?
○ Less than 1 year ○ 1 - 5 years ○ 6 - 10 years ○ 11 - 15 years
○ 16 - 20 years ○ 21 - 25 years ○ Over 25 years

3. What is the approximate number of your organization's employees AT ALL LOCATIONS?
○ 1 - 25 ○ 26 - 50 ○ 51 - 100 ○ 101 - 250 ○ 251 - 500
○ 501 - 1,000 ○ 1,001 - 5,000 ○ 5,001 - 10,000 ○ Over 10,000 ○ Unsure

4. What was your organization's total revenue (in pesos) in the past year?
○ Under 1 Million ○ 1 Million - 100 Million ○ 100 Million - 500 Million
○ 500 Million - 1 Billion ○ Over 1 Billion ○ Unsure

5. Do you supervise employees in your current position?
○ Yes ○ No

6. Which best describes your current position?
○ Senior Management ○ Front Line Management ○ I.T. Specialist
○ Middle Management ○ Administrative / Clerical ○ Other

7. What is your gender?
○ Female ○ Male

8. What is your age group?
○ Under 25 ○ 25 - 30 ○ 31 - 39
○ 40 - 49 ○ 50 - 65 ○ Over 65

9. What is the highest education level you have attained?
○ Some College ○ Some Graduate Work ○ Associate Degree
○ Bachelor's Degree ○ Master's Degree ○ Doctorate

10. How long has your organization been connected to the Internet?
○ Less than 1 year ○ 1 - 2 years ○ 2 - 5 years
○ 5 - 10 years ○ Over 10 years ○ Unsure

Section II - Internet Access

Please note that the term "Internet" as used in the succeeding sections of the survey refers to e-mail, web browsing, instant messaging, the use of Netmeeting, File Transfer Protocol (FTP), Telnet, news/stock tickers and other online activities.

11. Top management thinks I should use the Internet access facilities available at work in the performance of my job.

○ Yes ○ No ○ Do not know

12. Top management does not mind if I use the Internet access facilities available at work for personal, non-work-related activities.

○ Yes ○ No ○ Do not know

13. My immediate supervisor thinks I should use the Internet access facilities available at work in the performance of my job.

○ Yes ○ No ○ Do not know

14. My immediate supervisor does not mind if I use the Internet access facilities available at work for personal, non-work-related activities.

○ Yes ○ No ○ Do not know

15. I would be a more effective / productive employee if I had access to the Internet while at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

16. My Internet access at work allows me to engage in the following activities (Check all that apply):

○ Send/receive e-mail ○ Browse web sites ○ Send/receive instant messages ○ Chat ○ Download files

○ Participate in online bidding or auctions ○ Transact business with suppliers ○ Transact business with customers ○ Search for information ○ Read news, stock quotes

17. My Internet access at work is monitored.

○ Yes ○ No ○ Do not know

If you answered YES to question 17, please answer questions 18 -26.
If you answered NO or DO NOT KNOW to question 17, please answer questions 27-35

18. My organization has the right to monitor my Internet access at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

19. Monitoring Internet access at work violates my right to privacy.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

20. I would not abuse Internet access at work even if it was not monitored.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

21. I can be held liable for any illegal online activity I engage in while using the Internet access facilities at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

22. My organization can be held liable for any illegal online activity I engage in while using the Internet access facilities at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

23. My organization owns my email and any document I send, receive, download or otherwise access using the Internet access facilities available at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

24. My organization has the right to read my incoming and outgoing email if it deems it necessary.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

25. My organization has the right to block access to sites on the World Wide Web.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

26. My organization has the right to determine who is given Internet access at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

After answering questions 19-26, please answer questions 36-47 in Section III. Thank you.

27. I believe my organization has the right to monitor my Internet access at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

28. I believe monitoring Internet access at work would violate my right to privacy.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

29. I believe I would not abuse Internet access at work even if it was not monitored.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

30. I believe I can be held liable for any illegal online activity I engage in while using the Internet access facilities at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

31. I believe my organization can be held liable for any illegal online activity I engage in while using the Internet access facilities at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

32. I believe my organization owns my email and any document I send, receive, download or otherwise access using the Internet access facilities available at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

33. I believe my organization has the right to read my incoming and outgoing email if necessary.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

34. I believe my organization has the right to block access to sites on the World Wide Web.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

35. I believe my organization has the right to determine who is given Internet access at work.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

After answering questions 27-35, please answer questions 36-47 in Section III. Thank you

Section III - Internet Usage

36. Using the Internet at work has allowed me to better balance my work and personal life.

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

37. I allow work to follow me home — I forward office email to my personal email account.

○ Never ○ 1 - 4 times a year ○ 1 - 4 times a month ○ 1-4 a week ○ Everyday

38. I allow work to follow me home — I conduct online meetings with colleagues from other time zones from my residence.
○ Never ○ 1 - 4 times a year ○ 1 - 4 times a month ○ 1-4 a week ○ Everyday

39. I believe it is alright to use the Internet for personal, non-work related activities.
○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

40. The average number of hours I spend per week using the Internet access facilities for work is:
○ 1 - 5 hours ○ 6 - 10 hours ○ 11 - 15 hours ○ 15 - 20 hours ○ Above 20 hours

41. The average number of hours I spend per week using the Internet access facilities at work for personal, non-work-related activities is:
○ 1 - 5 hours ○ 6 - 10 hours ○ 11 - 15 hours ○ 15 - 20 hours ○ Above 20 hours

42. I use the Internet for personal, non-work-related activities more than I should.
○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

43. I believe that people in my organization use the Internet access facilities at work for personal, non-work-related activities more than they should.
○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

44. In the past month, I sent and / or received non-work related email while at work.
○ Never ○ 1-5 Times ○ 6-10 Times ○ 11-15 Times ○ Over 15 Times

45. In the past month, I have accessed the Internet for non-work-related activities while at work.
○ Never ○ 1-5 Times ○ 6-10 Times ○ 11-15 Times ○ Over 15 Times

46. In the past month, I have purchased a non-work related item via the Internet while at work.
○ Never ○ 1-5 Times ○ 6-10 Times ○ 11-15 Times ○ Over 15 Times

47. In the past month, I have downloaded files (programs, music, etc.) for personal use while at work.
○ Never ○ 1-5 Times ○ 6-10 Times ○ 11-15 Times ○ Over 15 Times

Section IV - Internet Usage Policy

48. My organization has an Internet Usage Policy.
○ Yes ○ No ○ Do not know

*If you answered **YES** to question 48, please answer questions 49 - 55*
*If you answered **NO** or **DO NOT KNOW** to question 48, please answer questions 56-62*

49. Agreeing to my organization's Internet Usage Policy was a condition of my employment or continued employment.
○ Yes ○ No ○ Do not know

50. I would agree to my organization's Internet Usage Policy even if it wasn't a condition of my employment or continued employment.
○ Yes ○ No ○ Do not know

51. The last time I read my organization's Internet Usage Policy was:
○ Never ○ 1-3 months ago ○ 4-12 months ago ○ 1-2 years ago ○ Do not know

52. My organization's Internet Usage Policy is enforced across all levels of the organization.
○ Yes ○ No ○ Do not know

53. My organization makes a sustained effort to ensure that all employees abide by its Internet Usage Policy.
○ Yes ○ No ○ Do not know

54. My organization disciplines any user who doesn't abide by its Internet Usage Policy, regardless of rank or position.

o Yes o No o Do not know

55. Overall, I believe that an Internet Usage Policy is an effective way to eliminate or at least reduce personal Internet and e-mail usage at work.

o Strongly Disagree o Disagree o Neutral o Agree o Strongly Agree

Thank you for your participation in this survey. Your candid answers to the preceding questions will go a long way towards understanding the effect of Internet Usage Policies in organizations.

56. In the event that my organization imposes an Internet Usage Policy, I would abide by the terms of the Policy if it was made a condition of my employment (or continued employment).

o Yes o N o o Do not know

57. In the event that my organization imposes an Internet Usage Policy, I would abide by the terms of the Policy even if it was NOT a condition of my employment (or continued employment).

o Yes o N o o Do not know

58. In the event that my organization imposes an Internet Usage Policy, I will need periodic reminders about the policy.

o Never o Every 1-3 months o Every 4-12 months o Every 1-2 years o No Opinion

59. In the event that my organization imposes an Internet Usage Policy, I believe that it should strictly enforce the policy across all levels of the organization.

o Yes o No o Do not know

60. In the event that my organization imposes an Internet Usage Policy, I believe that it should make a sustained effort to ensure that all employees abide by the terms of the policy.

o Yes o No o Do not know

61. In the event that my organization imposes an Internet Usage Policy, I believe that it should discipline any user who doesn't abide by the terms of the policy, regardless of rank or position.

o Yes o No o Do not know

62. Overall, I believe that an Internet Usage Policy is an effective way to eliminate or at least reduce personal Internet and e-mail usage at work.

o Strongly Disagree o Disagree o Neutral o Agree o Strongly Agree

Thank you for your participation in this survey. Your candid answers to the preceding questions will go a long way towards understanding the effect of Internet Usage Policies in organizations.