Acceptable use policy and employee computer usage: case of Sri Lankan software development industry

ACCEPTABLE USE POLICY AND MISUSE OF WORK COMPUTERS: CASE FROM SRI LANKAN SOFTWARE DEVELOPMENT INDUSTRY

Liyanagunawardena T. R.[1]
Samarasinghe K.[2]

ABSTRACT

Organizations introduce acceptable use policies to deter employee computer misuse. Despite the controlling, monitoring and other forms of interventions employed, some employees misuse the organizational computers to carry out their personal work such as sending emails, surfing internet, chatting, playing games etc. These ac-tivities not only waste productive time of employees but also bring a risk to the organization. A questionnaire was administrated to a random sample of employees selected from large and medium scale software development organizations, which measured the work computer misuse levels and the factors that influence such behavior. The presence of guidelines provided no evidence of significant effect on the level of employee computer misuse. Not having access to Internet /email away from work and organizational settings were identified to be the most significant influences of work computer misuse.

Keywords: Work Computer Misuse, Usage Guidelines

1. INTRODUCTION

Misuse of organizational information resources by employees is widespread and is increasing in frequency. Annual cost of computer crime is estimated to be in billions of dollars (Kreie and Cronan 1998). An article in Fortune magazine reported that many companies do not report such problems to avoid harmful publicity (Kreie and Cronan 1998). Even then there are many incidences of misuse of computers at work place that are reported.

Chevron Corporation had paid $2.2 million to female employees to settle a dispute regarding offensive emails circulated within the company by male employees that contained in one: “25 reasons why beer is better than women” (Zetter 2007). According to Industry Week, West Coast Company had paid $250 000 to settle an age discrimination law suit due to an email sent by its CEO, while the software giant Microsoft Corporation paid $2.2 million in a sexual harassment law suit involving pornographic message sent within company via email (Verespej 2000).

The increase in misuse of Information Technology resources at work place is a growing concern to organizations around the world. These activities increase the organizational expenditure, reduce the employee productivity, damage company reputation and may also result in security issues and legal liabilities (Zhang, Oh and Teo 2006; Zetter 2007). However, the losses due to computer misuse and computer crime have not yet attracted the attention of the corporate sector in Sri Lanka. In addition, it is observed that only little attention is paid to formulate appropriate policies to protect organizations from employee computer misuse amidst increasing number of information technology workers over the past few years.

There are several strategies used by employers to reduce employee computer misuse. Surveillance systems and continuous monitoring are being used by employers around the globe to spy on their employees computer use (Zetter 2007; Schulman 2001). Adopting policies is another method used by organizations to deter employee computer misuse (Case and Young 2002; Lichtenstein and Swatman 1997).

In order to curb employee computer misuse, it is necessary to identify the factors influencing such activities. Further the role played by policies in deterring misuse and their effectiveness should be explored in order to formulate strategies to be recommended for the employers. This study investigates the factors influencing employee computer misuse in medium and large scale software development organizations .

2. PREVIOUS WORK

Employee computer misuse has become a burning issue for the employers, and several research have

1 Department of Computer Science and Engineering University of Moratuwa, Sri Lanka (t.liyangunawardena@gmail.com)

2 Department of Electronics and Telecommunications Engineering - University of Moratuwa (kithsiri@ent.mrt.ac.lk)

investigated this issue during the past years.

2.1 Information System Misuse

Information system misuse and computer crime is defined as: "unauthorized, deliberate and internally recognizable misuse of assets of the local organizational information system by individuals. Possible abuses include violations against hardware, programs, data and computer services" (Straub, cited in Foltz, Cronan and Jones 2005). This definition covers all the major areas of computer systems, hence can be considered as a general definition for the computer misuse. However, many definitions can be found in information system misuse literature. Downloading copyrighted material, child pornography, employee sabotage and misappropriation of confidential information are defined as misuse of employer technology by Totten (2004).

Misuse of computers at workplace can be seen in many areas. The Internet misuse is one of the key areas that affect organizations. This is mainly because internet misuse not only reduces the productivity of employees but also brings in a risk to the organization. Activities such as participating in chat rooms, slacking (stocks, surfing, sports, news groups), cybersex, pornography and gambling are some of the internet misuses that can be seen at work. Sexual harassment, cybersex and pornography can be classified as extreme negative behaviors because of their inherent legal implications (Case and Young 2001; Zetter 2007). Furthermore, pornographic, gambling and gaming sites can harbor viruses and other malicious programs that would allow outsiders to damage private networks or make off with sensitive information compromising the network security (Zetter 2007). Marson (2000) points out that there had been an increase in the use of work hours to earn money by searching the web or winning sweep stakes. According to a survey by Nielsen/NetRatings, during the month of January, 7,000 employees in the survey spent an average of 67 minutes at iWon.com, one of the top 10 sites where employees spent the time most.

Email has become an integral part of the professional life and an indispensable element of business communications. "The Federal Bureau of Investigations (FBI) and the Computer Security Institute's 2001 Computer Crime and Security Survey found that 91% of participating computer security practitioners detected employee abuse of internet access privileges at their work place including inappropriate use of email systems" (Mastrangelo, Everton and Jolton 2006).

A 2005 survey by salary.com and America Online found that employees on average waste at least two hours a day (much of it online) performing things other than work, at an annual cost to business of about $759 billion (Zetter 2007).

2.2 Consequences of Misuse

It is evident that misuse of computers at work place is more than just time wasting. Monitory loss to businesses as a result of the misuse of computers and computer fraud amounts to billions of dollars per year (Kreie and Cronan 1998). Furthermore, the negative publicity for any incident would tarnish the image of the organization.

The Internet misuse alone has several impacts upon organizations, namely: issues related to the drain on telecommunications bandwidth, legal liability, security of company data and ultimate loss of productivity. The concern about the Internet abuse and the associated legal liabilities, negative publicity and excessive costs are consistent across industries and company size (Case and Young 2001).

Work computer misuse has led to employee discipline and termination. Xerox Corp., The New York Times, and First Union Bank have announced termination of employees for inappropriate Internet use (Verespej 2000). PNC Bank in New Jersey sacked two long time workers who did not comply with the bank's formal policy against internal distribution of offensive material (Zetter 2007).

2.3 Controlling Misuse

According to Case and Young (2002) there are two primary tools that Information Systems (IS) department may employ to combat the internet misuse. Those are monitoring and utilizing an Internet use policy.

Increasing number of companies invest on employee monitoring devices as it is believed to be an easy way to reduce employee misbehavior, competitive information leaks and liability risks (Enbysk n.d). In the United States, there is fourteen million employee's Internet or email use under continuous surveillance. Further, it is argued that the systematic monitoring raises much larger privacy issues than spot checks. "One reason for monitoring all employees without individual suspicion is that, in a way, the entire work force is under suspicion" (Schulman 2001). However, it is also identified that this type of surveillance will inject an air of suspicion and hostility to the work environment.

Despite the level of surveillance, many employees continue to use their computers at workplace for a wide range of personal activities ranging from

sending personal emails, instant messaging, word processing to online shopping. Survey of computer use at work carried out by WeComply Inc. New York reveals that majority of the employees do not realize that personal web searches, instance messaging to friends on their work computers could become business records (WeComply Inc.2007). Therefore it can be interpreted that increasing awareness is a must in handling employee computer misuse.

"A policy is a broad guideline for decision making that links the formulation of strategy with its implementation" (Wheelen, Hunger and Rangarajan 2006, p.13). Policies are typically instituted in order to avoid some negative effect that has been noticed in the organization, or to seek some positive benefit.

Employing an acceptable use policy at work to deter computer misuse is suggested by many studies. (Case and Young 2002; Lichtenstein and Swatman 1997). An Acceptable Use Policy (AUP) is defined as a policy which contains guidelines for the employees including both acceptable and unacceptable uses, with the aim of controlling those employee behaviors and actions that contribute to the organization's risks, while maximizing the employee productivity (Lichtenstein and Swatman 1997). In every contract of employment, there is an unwritten, mutual trust between both parties; employer and employee. More formally most companies opt for an acceptable use policy signed by employees before they are permitted to use the employer's network resources (Stephan and Petropoulakis 2007).

Using written statements to reduce the occurrence of some undesirable action is based on the Theory of General Deterrence, which suggests that punishing offenders will prevent others from same behavior (Harrington 1996). The awareness of consequences for a behavior could alter how the people behave. Therefore the management could very likely affect behavior of employees by making a clear statement of policy and expectations of what behavior is unacceptable and the consequences for such behavior (Kreie and Cronan 1998). "The development of ethical standards and regulations that are perceived as acceptable and appropriate by the majority of users is needed to facilitate compliance with legislation and with company and industry policies for the ethical use of computer technology" (Gattiker and Kelley 1999).

Several professional organizations including IEEE and ACM have developed professional codes of ethics to cope with problems associated with unethical use of computer technology (Walsham 1996). Therefore it is evident that IS professionals, organizations and research have identified formal computer guidelines as an effective method of eliminating or at least reducing misuse of computer technology.

2.4 Acceptable Use

Defining an "Acceptable Use" for an information technology oriented organization is not an easy task. According to Pierce and Henry (2000) it is difficult to give a definitive statement of "acceptable behavior" and thus difficult to write specific codes as computer technology environment is changing very rapidly. Although the term misuse may be applicable in the sense that the employee deviate from employer's expectation of work behavior, some form of use may indirectly maximize employee performances by releasing them from stress or improving knowledge which intern will help the organization.

However a total ban on personal use of the internet may cause resentment or indeed strong protest from employees. The culture will have an influence on the amount and types of freedom which employees expect. Therefore having internet user etiquette to suit its peculiar culture with in the acceptable use policy can be considered (Lichtenstein and Swatman 1997).

When faced with an ambiguous ethical situation related to computer technology, an individual's course of action is influenced by personal experiences and opinions, consideration of what co-workers would do in the same situation, and an expectation of what the organization might sanction (Pierce and Henry 2000). Therefore it can be seen that a clear policy on acceptable use would guide the employees in resolving the ambiguousness. However the policy needs to be well written, considering all aspects in order to have better results. It is identified that implementing controls, as identified in a policy, would indeed deter computer misuses (Dhillon 1999).

2.5 Effectiveness of Acceptable Use Policy

Whether computer guidelines have been an effective deterrent in combating unacceptable use of work computers need to be revisited. A study done by Vitell and Davis (1990) have concluded that the existence of codes of ethics and the ethical actions of top management are perceived by MIS professionals as having very little impact upon either "opportunities for" or the "frequency of" unethical behavior. However in Vitell and Davis's study (1990) only 13.1% of the respondents reported that their company had a formal, written code of ethics. Therefore it can be also argued that the acceptable use policies were only getting implemented at that time and most likely that the acceptable use policies have not being covering all the aspect that they needed to cover.

A more recent study by Foltz, Cronan and Jones (2005) also concludes that mere presence of a computer usage policy does not make a difference in a university environment. However it was also identified in the research that the presence of a computer use policy does influence the students who have read the policy. This study concluded that the existence of computer use policies with in an organization does not ensure all users are familiar with the contents of those policies and the penalties imposed for their violation. Also it points out that providing a copy of computer use policies to employees and verbally highlighting major points is not sufficient exposure to eliminate indifference about computer misuse. It suggests that additional means are necessary for every member of an organization to gain appreciation of, to understand and to comply with computer usage policies.

Most of these research were performed on student samples. Due to their lack of professional experience using undergraduates as the sample and generalizing it to organizational employees is questionable. However in many studies undergraduates are used in evaluating ethical behaviors in computer use (Leonard and Cronan 2005; Kreie and Cronan 1998).

It is necessary that the computer use policy defines the consequences of not adhering as a separate section. This should not be used as a weapon to gun down an employee for the first violation but repeated offenders should be punished. Acceptable use policy violation investigations most of the time falls within the scope of the Information Technology department of an organization. But sharing the responsibility with the Human Resource Management department and Legal Department can also be considered (Lawrence n.d.).

2.6 Factors Influencing Computer Misuse

There are few recent studies carried out in the area of non work related use of Information Technology resources in the work place (Mastrangelo, Eerton and Jolton 2006; Zhang, Oh and Teo 2006). It is important to understand the factors influencing non work related use in making policies to deter misuse.

Mastrangelo, Eerton and Jolton (2006) have developed 'ABCD Model of Work Computer Deviance' which examines the 'Access to computers/ Internet', 'Breaks from Work', 'Organizational Climate' and 'Individual Differences' in the context of environmental and personal variables. Authors believe that this model covers majority of the factors that govern deviant use of computers by employees in the Sri Lankan context as well. In the above research under 'Access computers/ Internet' it was identified that participants gained more recent Internet access and participants with faster Internet access at work engage in deviant computer use. In the same study under 'Breaks from Work' it identified that the number of concurrent jobs has a relationship with work computer misuse. Above study revealed that the ethnicity of the users had no relationship with the deviant computer use. Under 'Organizational Climate', research has looked at evaluation of the job, learning one's organizational climate and knowledge of coworker being warned for misuse. 'Individual Differences' looked at age, gender and ethnicity.

According to the findings of Vitell and Davis (1990), IS professionals with higher income tend to be optimistic about success and ethical behavior. It is identified that universal moral beliefs to be a governing factor influencing employee behavior and individuals with a strong belief in universal moral rules exhibit higher ethical intentions regardless of whether or not computer guidelines were present (Peterson 2002). It is also stated that for those who do not believe strongly in universal moral rules, ethical intentions were high only when clear computer guidelines were available. Universal moral beliefs influence on employee behavior is also supported by Pierce and Henry (1996) in their study on the role of informal code, personal code and formal code on ethical behavior. Here the personal code of ethics referrers to the developed code by an individual from observation and experience. Informal code of ethics is the accepted behavior in the work place or peer expectations and the formal code of ethics is the company code or policy with provisions that apply to computer use.

Zhang, Oh and Teo (2006) have shown that anonymity and privacy to be factors of importance when it comes to non work related use of IT resources at work place.

Organizational Culture is 'the basic pattern of shared assumptions, values, and beliefs governing the way employees within an organization think about and act on problems and opportunities' (McShane and Glinow 2005, p. 16). The organizational culture has shown to have an effect on network based computer usage (Kanungo 1998). In the above study organizational culture was measured based on people orientation and task orientation. A more recent study states 'organizational culture would certainly influence the operation activities of an enterprise and the effectiveness of an enterprise's information security practice' (Chang and Lin 2007). It measured organizational culture based on 'Internal/External Orientation' and the 'Flexibility/Control Orientation'. Authors believe that this basis is more appropriate for measurement of organizational culture because information security practices have a close link to acceptable use policies as it can be considered one

way of implementing information security practices. McShane and Glinow (2005, p.446) defines Organizational Structure as the division of labour and the patterns of coordination, communication, work flow and formal power that direct organizational activities. Organizational hierarchy expansions or contraction to support controlling of misuse in organizations was proposed as formal intervention by Dhillon (1999). Therefore it is worthwhile to examine the organization's structure and whether it influences the misuse within the organization.

3. OBJECTIVES

The research is unique as it is investigating the effectiveness of acceptable use policies in deterring employee computer misuse in Sri Lankan context. Though there had been research studies investigating employee computer misuse and the effectiveness of acceptable use policies in other countries, research studies focusing on this area is scarce in Sri Lanka. Therefore a descriptive study followed by a correlational investigation was employed in this research to explore the factors influencing computer misuse. The main intention of this research is to delineate the important factors associated with the problem of work computer misuse.

4. RESEARCH METHODOLOGY

Work computer misuse have been studied earlier by several researchers (Mastrangelo, Eerton and Jolton 2006; Zhang, Oh and Teo 2006). Acceptable Use Policies have been in existence for many years and therefore they have been studied earlier (Lichtenstein and Swatman 1997; Peterson 2002; Case and Young 2002; Foltz, Cronan and Jones 2005). However since there has not been a comprehensive study on acceptable use policies in Sri Lankan context this opportunity will be taken to present the unique aspects of Sri Lankan situation using an Analytical and Predictive analysis.

4.1 Research Approach

A descriptive study was employed to provide a better understanding of acceptable use policy implementations in Sri Lankan software development organizations. The descriptive study is undertaken in order to ascertain and be able to describe the characteristics of the variables of interest in a situation (Sekaran 2006, p.121). Managers of the selected organizations were contacted to gather information regarding the availability of an acceptable use policy in their organizations governing employee computer use. Further where possible the acceptable use policies were studied in order to understand the coverage of them. However it was expected that there would be reluctance from managers of organizations which have not implemented Acceptable Use Policies, in revealing their organization's status as it would definitely be an unveiling of their vulnerability. Apart from analyzing organization's acceptable use policy, interviews with managers/team leads and email communications were employed to gather information.

The purpose of the study is hypothesis testing and the type of investigation is correlational. Since a correlational study is normally conducted in the natural environment of the organization with minimum interference by the researcher with the normal flow of work (Sekaran 2006, p.127), this study is also done in the natural environment of work. This approach is supported by the literature as surveys done in the natural environment have been the main research approach adopted by pervious researches (Vitell and Davis 1990; Case and Young 2002; Peterson 2002; Mastrangelo, Everton and Jolton 2006). Therefore the study setting is non contrived.

4.2 Theoretical Framework

Researchers were interested in identifying whether the existence of an acceptable use policy has any effect on the employee computer misuse. Therefore the a set of hypothesis was formulated as:

H_0: Acceptable Use Policy has no effect on employee computer misuse

Against the alternative

H_A: Acceptable Use Policy has an effect on employee computer misuse

Statistically H_0 says that the mean value of misuse is equal in organizations with acceptable use policy in existence and without.

According to the literature authors identified several factors that influence computer misuse at workplace. These factors can broadly be categorized into three. Individual differences as identified by Mastrangelo, Everton and Jolton (2006), Organizational settings and Situational influences. Figure 1 summarizes the factors being considered under each category.

The Instrument used in this research is a questionnaire where questions were composed to cover the factors that affect employee behavior in using work computers (as identified by the literature review) and to measure the employee computer misuse. Demographic details of the participants were also collected. Operationalization of the concepts and formulation of the questionnaire were done in

accordance with previous literature. (Pierce and Henry 1996; Mastrangelo, Everton and Jolton 2006)

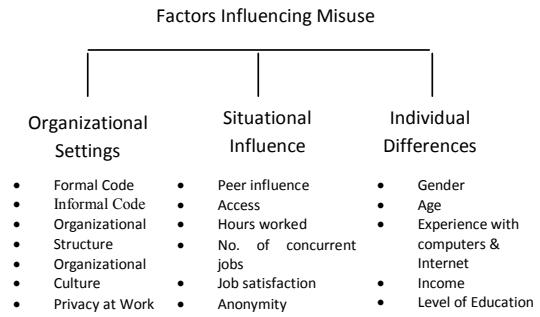

Figure 1: Factors Influencing Misuse

In designing the questionnaire each Likert scale item was given as a scenario where the subject was asked to mark the appropriate response from strongly disagree to strongly agree (the answers provided were strongly disagree, disagree, neither agree nor disagree, agree and strongly agree).

The dependant variable in this study is the employee computer misuse. As revealed from the interviews with higher management of software development organizations, computer use at work can mainly be divided into two from the point of view of the organization. First is the use of computers for work related activities while the other is the use of computers for non-work related activities. In a preliminary analysis of the acceptable use policies of software development organizations it was identified that each organization was specifically interested in employee's email, Internet and general computer use. Therefore these three areas were used to measure the computer misuse of employees. Per each of these areas questions were included in to the questionnaire. The questionnaire consisted of nine items covering all three areas, namely: email misuse, internet misuse and general computer misuse. The scenarios for misuse were developed using the deviant computer use items identified by Mastrangelo, Everton and Jolton (2006) and the "Don't s" sections of the analyzed Acceptable use policies. For example the sending of chain mails is prohibited or discouraged by most Acceptable use policies. Therefore the scenario "I use my office email to send/forward humorous materials or chain mails to friends" was developed.

A question was introduced to identify whether the organization possessed an acceptable use policy or not. In case the organizations possessed an acceptable use policy the subject was tested for the level of awareness about the use policy.

In measuring demographic items, the questions were placed at the bottom of the questionnaire under the assumption that the subject would be more comfortable in revealing that details once he/she is convinced of the legitimacy and genuineness of the questions framed by the researcher. With this idea the income of the subject was asked at the end of the questionnaire just before the demographic data collection section.

Universal moral belief of the subject was targeted by the question "I have a well formulated personal code of ethics related to computer use which guides my behavior at work" (Pierce and Henry 1996). If this question was answered with strongly agree then it would imply that the subject is having a high standard for ethical behavior. "I am aware of the specificity of the informal company code of ethics (Pierce and Henry 1996). (Here informal company code of ethics means the general work norms in the work place)" targeted the subject's awareness level of the informal code at the work place. Two questions were introduced to measure the level of addiction to computers/ internet. These had been used by Mastrangelo, Everton and Jolton (2006) in identifying addiction. Job satisfaction, peer influence were targeted by one question each while another was introduced to check the anonymity. Also one question was introduced to identify the level of privacy at work. Access to internet and email was targeted by two questions. To obtain the subject's level of experience with computers and email/internet two questions were introduced. Amount of work carried out was questioned using three questions in the form of one leading to the next. Four items were introduced to measure organizational culture, one per each cultural trait cooperativeness, innovativeness, consistency and efficiency as identified by Chang and Lin (2007). Organizational structure was measured using three questions which targeted the span of control , centralization and level of formalization. Here span of control referrers to 'the number of people directly reporting to the next level in the organizational hierarchy' (McShane & Glinow 2005, p. 449) and centralization referrers to the formal decision making authority held by a small group of people, usually those at the top of the organizational hierarchy (McShane & Glinow 2005, p. 451). Formalization is the extent to which organizations standardize behavior through rules, formal training, procedures and related mechanisms (McShane & Glinow 2005, p. 453). According to these three measures organizations were classified into 8 categories. Here the organizations with span of control less than 20 (as suggested by Henry Feyol in McShane and Glinow 2005) was taken as narrower span of control organizations. Organizations scoring greater than three on the likert scale for level of centralization were categorized to highly centralized organizations. Finally according to the response provided for Question "My organization is

a systematic organization where each employee has clear duty, and its operations are well defined with clear rules to follow" organizations which received more than three on the likert scale were considered to be formal organizations.

Table 1: Organizational Structure Categories

Organization Category	Level of Centralization	Span of Control	Level of Formalization
1	High	Wide	High
2	High	Wide	Low
3	High	Narrow	High
4	High	Narrow	Low
5	Low	Wide	High
6	Low	Wide	Low
7	Low	Narrow	High
8	Low	Narrow	Low

4.3 Sampling Design

4.3.1 Population

The population of this study is the employees of medium and large scale software development organizations in Sri Lanka.

Rationale

Sri Lanka Association for Software Industry (SLASI) and Software Exporters Association (SEA) are the most reputed member associations in Sri Lanka for the software industry. According to their member information there are about 100 software development organizations. However in total there are about 170 software development organizations in Sri Lanka. Out of these most of the companies have less than 30 employees and are still in their infancy. Case and Young (2002) had identified that the Organizational size has a co-relation with the implementation of acceptable use policies. Therefore authors contacted few of these start up companies in order to find information about the level of formalization of these organizations. There it was understood that these organizations were not at all formalized. They had limited number of employees whom they trusted and had control over. Therefore authors narrowed down the population to be 'employees of medium and large scale software development organizations in Sri Lanka'. Here the terms 'medium' and 'large' needed to be defined. Business sector in Sri Lanka is divided into sectors using different criterion by different institutions. Some of the criterions used are: amount of capital invested, amount of turnover, the nature of the business and number of persons employed (Kapurubandara and Lawson 2006). However according to the above mentioned criterion the amount of capital invested and amount of turn over can not be practically used in this study because most Sri Lankan software development organizations are private limited companies where the financial statements are not available for the general public. This limitation will hinder the quality of information that is available for this study. The nature of the business can not be taken as the criteria as the study is focusing on only one sector. Therefore the final criterion 'number of persons employed' was used to make the distinction between the organizations.

In Sri Lanka the Department of Census and Statistics, Small and Medium Enterprise Development, and the Federation of Chambers of Commerce and Industry use the number of employees as the criterion to categorize organizations as large, medium or small (Kapurubandara and Lawson 2006). The Asian Development Bank defines enterprise size in Sri Lanka based on the number of employees: those with 5- 49 employees are small; those with 50-149 employees are medium-sized; and those with more than 150 employees are large (Asian Development Bank 2001). According to the above definition, the employees of software development organizations with 50 or more employees were considered the population. The target population consisted of 30 software development organizations with around 4300 employees.

Considering the above population frame it was required to design the sampling. According to the objectives of this research it is required to compare the computer use of employees of organizations with acceptable use policies in existence and without. Therefore authors contacted each of these eligible organizations to gather information regarding the existence or non existence of an acceptable use policy in the organization. At this point it was evident that some of the organizations immensely resisted revealing this information. Therefore the number of organizations considered for this research was reduced to the ones that provided the information. In a few instances organizations provided the required information requesting for a guarantee that the organization name would not be revealed in the study. In order to minimize the bias due to non responsiveness, authors informally approached the organizations that expressed their reluctance to respond. Then it was revealed that most of the organizations that did not respond have not employed an acceptable use policy. By revealing the fact that an acceptable use policy is not in place would have placed these organizations in a disadvantageous position. Further it was also revealed that some of the organizations were actually in the process of formalizing the procedures.

4.3.2 Sampling

It is obvious that the culture, structure and work practices of organizations differ from one to another. Therefore to gather overall picture it is vital to design the sampling in a way that it represents the whole population. When there are identifiable subgroups of elements within the population that may be expected to have different parameters on the variables of interest to the researcher stratified random sampling is preferred (Sekaran 2006, p. 271). Therefore stratified random sampling method was selected as the sampling method to draw a representative sample from the population. Stratified sampling involves a process of stratification of population into mutually exclusive sub groups. Here the stratification was done based on the organization. Since one employee could only be employed full time in one organization the stratification divided the population in to mutually exclusive sub groups. Random sampling method was selected over non-probability sampling to achieve least bias and most generalizability.

4.3.3 Procedure and Pretest

The draft questionnaire was prepared and it was pretested by administrating to a group of 15 individuals from different demographic backgrounds.

The pretest revealed that some of the individuals were not aware of the acceptable use policy of the organization even though it existed. Therefore it was required to collect the organization's name along with the question whether the organization possessed an acceptable use policy in order to validate the data. This was the most valuable input that was extracted out of the pretest which would have otherwise lead to invalid data in analysis.

As the organization name needed to be given in the questionnaire due to the above reason, most of the subjects who were involved in pretest did not reveal their designation. When asked about the non responsiveness the majority felt that revealing their company name and designation along with the income would violate the company policy of non disclosing salary information. 90% of the pretest sample revealed that out of these questions (Company Name, Designation and Income) they would only respond to maximum of two questions. Since organization's name was required to filter out the invalid responses and the income was required as it was identified to be an influencing factor for employee computer misuse, the only option was to leave out the question which targeted the designation merely to collect demographic details.

Each of the eligible organizations was contacted and a person was appointed for each organization. The appointed person was briefed on how to randomly select individuals from the organization to administer the questionnaire. Telephone conversations, email communications and meetings were used in order to educate the appointee. The questionnaire was emailed to the subjects through the appointed person for that organization. An email account was created and its details were published with the questionnaire for the respondents' use in case they preferred anonymity. Authors administrated the questionnaire in one organization. Both printed and email questionnaires were used to gather data in this research.

4.3.4 Sample

The total number of responses received was 91 out of which 3 had to be discarded due to missing data and subjects not being aware of the existence of the use policy in the organization. Therefore final usable responses amounted to 88.

Out of these 88 responses 28 were from female respondents. However considering the current composition of IT workforce in Sri Lanka which has only 21% females (Sri Lanka Information and Communication Technology Association 2007) the sample representative ness of females was acceptable. Educational back ground of the sample can be summarized as follows: 80% of the sample was graduates and 17% had postgraduate qualifications. 3% of the sample had only A/L as the highest educational qualification. Mean age of the respondents was 28.26 with a standard deviation of 3.675. The sample consisted of 39 subjects from organizations which had employed acceptable use policies and the remaining 49 subjects were from organizations which had not employed acceptable use policies. Employees from 25 organizations (out of the eligible 30 organizations) took part in this study. Details of sample demographic details are provided in Appendix - A.

5. RESULTS AND DISCUSSION

5.1 Reliability

The interim consistency reliability or the Cronbach's Alpha reliability coefficient of the preliminary variables were calculated to investigate the reliability of data. In general, Cronbach's alpha in the 0.70 range is considered as acceptable (Sekaran 2006, p. 311). The calculated Cronbach's alpha for the dependent variable of the study (misuse) was 0.728, which suggested that the reliability of the measure was acceptable.

Table 2: Reliability Statistics

Cronbach's Alph	No of Items
0.728	9

5.2 Analysis of Data Distribution

The most important variable in this study is the level of misuse of work computers. The distribution of the variable was investigated to identify whether it was normally distributed as identification of the distribution is vital for further statistical analysis. Chi-Square test was used to test whether the values were normally distributed with the following hypothesis.

H_1 : The data is normally distributed
Against the alternative
H_{1A}: Data is not normally distributed

The Chi-Square test was applied and a p-value of 0.0664 was obtained. Since this is greater than 0.01, H_1 was accepted. That is the data is normally distributed. Therefore further statistical tests were selected as appropriate.

5.3 Analysis and Discussion

The preliminary investigations revealed that out of the responded organizations only eight organizations possessed some form of a written guideline. It was also observed that out of the large scale organizations 80% of organizations possessed a guideline to guide employee computer use while only 18.18% of medium scale organizations possessed the same. This observations are consistent with the observations made by Case and Young (2002) in suggesting organizational size has a co-relation with the implementation of acceptable use policies.

Authors were able to access five acceptable use policies from these organizations. Since most of these organizations were private limited liability companies, organization's management treat these policies as strictly confidential. Only one organization had its acceptable use policy publicly available on the internet. This organization is a higher educational institute which comprises of a software division. Most of the studied acceptable use policies were not comprehensive in defining acceptable use and non acceptable use. There were some policies with ambiguous statements. For example one acceptable use policy contained the statement "Employees are responsible for exercising good judgment regarding the reasonableness of personal use". One organization possessed an acceptable use policy which could be taken as a comprehensive guideline in all aspects of computer usage. Software, hardware, general computer use, network use and internet/email use was covered in this policy. This organization is a branch of a larger organization which has a global presence. In this policy they have specifically mentioned that internet use for personal reasons and playing of games is not allowed during office hours. However they also mention "playing of computer games outside work hours and on holidays is not discouraged..." and "Internet access for personal needs with in the parameters outlined in the section on 'Internet and Email Policy' should be done outside working hours and on holidays to reduce the network traffic sustained during working hours.". This policy does allow internet use for personal reasons to some extent within a boundary defined by the organization. As suggested by Lichtenstein and Swatman (1997) a total ban on personal usage of internet may cause strong protest from employees. By giving some consideration to this issue and developing the acceptable use policy of the organization would make it more accepted by the employees. However most institutes strictly prohibit the use of organizational IT resources for personal gain.

Information and Communication Technology Agency of Sri Lanka has recently formulated the Information Systems Acceptable Use Policy for the government organizations (Information and Communication Technology Agency of Sri Lanka 2005). It is very encouraging to see a government agency taking a step ahead of most private organizations in leading the way to make acceptable use policy a standard practice. Currently the third version of the policy is in effect and it clearly states that the usage of information systems resources is for business purpose only.

5.3.1 Effectiveness of Acceptable Use Policy

When analyzing misuse a mean value of 29.30 with a standard deviation of 5.53 was obtained on a scale of 9-45 for employees of organizations with acceptable use policies in existence. Mean of 30.12 with a standard deviation of 5.8 was obtained for employees of organizations without acceptable use policies. By applying t – test for the misuse, t value of 0.67 was obtained meaning that the level of misuse in organizations with acceptable use policies in existence and without are equal at 5% level. Therefore the null hypothesis H_0, that is: 'Acceptable Use Policy does not make a difference in employee computer misuse' was accepted.

According to this observation the presence of an acceptable use policy shows no effect on employee computer misuse behavior. Even though this is an overwhelming observation the reality out there is being revealed in the study. Also this is not the first instance that this kind of an observation was made. In a previous study Vitell and Davis (1990) have

concluded that the existence of codes of ethics and the ethical actions of top management are perceived by MIS professionals as having very little impact upon either "opportunities for" or the "frequency of" unethical behavior. A more recent study by Foltz, Cronan and Jones (2005) also concluded that mere presence of a computer usage policy does not make a difference in a university environment.

Each of the misuse scenarios was then analyzed to explore whether there were any differences between the two groups of employees in specific scenarios. Firstly Chi-Square test was applied to investigate whether the responses for each question were normally distributed. Since they were not normally distributed Mann-Whitney U test which is a non parametric test was used. Here the Null hypothesis was the responses for each question in the two groups has the same distribution against the alternative that they are different. According to the results the null hypothesis was accepted in all cases except for one. This implies that there is no significant difference in the responses of either group for eight out of nine scenarios being presented to measure the level of misuse. The analysis revealed that there is a significant difference in the case of one scenario even at 1% level.

Table 3: Mann- Whitney U Test Results

Misuse Question Number	Mann-Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	952.5	1732.5	- 0.027	. 978
2	797.0	1577.0	- 1.376	.169
3	797.5	2022.5	- 1.512	.131
4	681.5	1906.5	- 2.456	.014
5	770.5	1995.5	- 1.721	.085
6	880.5	2105.5	- 0.677	.498
7	839.0	2064. 0	-1.042	.298
8	845.5	1625.5	-.958	.338
9	803.0	2028. 0	-1.365	.172

For questions see Appendix – B.

Under these observations it is worthwhile to recall this scenario. The scenario asked the subjects "I have downloaded music/pictures/software using office internet connection". For this question, employees of organizations with acceptable use policies in existence responded with a mean value of 3.2 while the other group responded with a mean value of 3.7. With 99% confidence it can be said that the employees of organizations with acceptable use policies in existence and employees of organizations with no acceptable use policy in existence behave differently with respect to this scenario. By analyzing mean value of each group it was evident that employees of organizations with acceptable use policies in existence were more cautious in downloading music/ pictures / software using the office internet connection. This can be due to the specific guidelines given in acceptable use policy regarding downloading of material from internet. Almost all the policies studied had some form of guideline covering the downloading of music and/or software using office internet connection. For example this was one guideline provided by an organization regarding downloading of material from internet. "When downloading software, please comply with Company 'A' procedures for the importation of software, even if it is a 'public domain'. As a courtesy to others, try to do large file transfers during off hours for the server." Downloading of music, software or pictures eat up the bandwidth of the connection causing heavy network traffic. Further downloading of copywrited materials, pornography can cause legal liabilities while bringing in a risk due to virus threats coming into the network. Therefore it is evident that organizations that have employed acceptable use policies enjoy a productive network usage compared to their counter part.

The factors identified to influence employee computer misuse were tested using appropriate statistical methods to check their significance. ANOVA and correlation investigations were employed in investigating these. Only few factors provided evidence to conclude that they were significant in influencing employee computer misuse.

Statistical tests revealed that 'Access' had an influence on level of employee computer misuse. Analysis for variance indicated that there is a significant difference between the two groups even at 1% level. People who have email and internet access away from work and people who do not have internet/email access away from work showed significant difference in the level of misuse of work computers. Former group engaged in less misuse.

Table 4: ANOVA Results for Access and Misuse

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	333.747	1	333.747	11.707	0.001
Within Groups	2451.696	86	28.508		
Total	2785.443	87			

According to the observations made it was clearly visible that not having access to internet/email out side the work place makes employees engage in more misuse. This can be expected as the employees would try to browse the internet for personal reasons during work hours using office internet connection as they do not posses the luxury to do so away from work. This observation differs from the observations

made in the previous researches being carried out in the area of work computer misuse. Mastrangelo, Everton and Jolton (2006) have rejected the hypothesis "participants who only have internet access at work will report more deviant computer use than participants who have access outside of work". However they have observed employees engage in more misuse when they have faster internet connections at work than at home. In Sri Lanka majority of employees use dialup connections to get connected to the internet. Only 6 subjects (out of 91) of the study had indicated that they have unlimited access as they have an Asymmetric Digital Subscriber Line (ADSL) connection. Therefore it is obvious that almost all other participants of this research have slower internet connections than they have at work.

According to the department of census and statistics the percentage of households with internet facility is 0.7% and the percentage of households with email facility is 0.9% (Department of Censes and Statistics - Sri Lanka 2004). Above statistics reveal that only a smaller portion of workforce has access to internet, email away from work. It is required to provide access to internet, email to the community at large in order to pave way to a information society. Some organizations have initiated this by providing ADSL connections to their staff. However these facilities are mostly given to managers and not to the mass of employees. Due to the penetration of Code Division Multiple Access (CDMA) phones in the island one can argue that it is possible to get connected to internet. However the charges for internet connectivity are based on two components most of the time. Internet account is charged at one rate and the call to make the connection is charged based on local call rates. An ADSL connection through Sri Lanka Telecom costs Rs 2250/= per month which is a considerable cost for a consumer. On the other hand by using Rs. 200/= prepaid card from Sri LankaTelecom a consumer can surf the internet for 10 hours at the rate of Rs 20/= per hour (Sri Lanka Telecom nd). If a concessionary flat rate could be considered for the use of internet this would help users to access internet without the fear of getting high phone bills. During the informal interviews with employees of software development organizations it was revealed that even though they had phone connection and a personal computer at home they did not want to access internet as they feared getting higher phone bills. One said "time passes quickly when you are surfing. If I were to use internet from dialup connection I would end up paying my whole salary for the phone bill".

The variance of misuse in each of the different organizational categories was checked to see whether there was significance.

Table 5: ANOVA for Org. Category And Misuse

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	637.456	7	91.065	3.392	0.003
Within Groups	2147.987	80	26.850		
Total	2785.443	87			

According to table 5 it is evident that there is a significant difference between the levels of misuse in different organizational structures even at 1% level. Therefore the data needed to be further analyzed to explore the relationship between organizational structure and the level of misuse. For this the Tukey Pairwise Comparison test was used. The test revealed that the difference in mean was significant at 5% level between organizational category 3 and category 6. Organizations categorized under category 3 have high centralization, narrow span of control and high formalization. On the other hand categorization 6 is for organizations with low centralization, wide span of control and low formalization showing exactly the opposite characteristics of category 3. Also it can be seen that the organizations having characteristics of category 3 enjoy less misuse than their counterpart.

Therefore it is evident that less misuse is observed in places where close monitoring and control is seen. The clear indication of positional power in a centralized decision making authority may influence the behavior of the employees. Also the close monitoring that can be seen with narrower span of control structures may not leave room for employees to engage in misuse of work computers in the work place. This fact is important to all software development organizations in Sri Lanka as most of the organizations are structured in flat wide span of control structures as opposed to tall structures with narrow span of control. Therefore it is required to take necessary steps to reduce the level of employee computer misuse in these companies by employing appropriate policies, procedures, monitoring etc.

The data provided evidence to conclude that peer influence has significance in influencing work computer misuse. The correlation was weak (0.456) but significant even at 1% level.

None of the other factors that were identified to be influencing misuse in previous researches significantly contributed in Sri Lankan case. For example "Non productive computer use is far more prevalent and consists of time spent socially connecting or engaging in activities unrelated to work. This use is more common among younger employees, males, and those who use computers compulsively" (Mastrangelo, Everton and Jolton 2006). Current research did not

provide evidence to support any of the above factors. Further privacy at work place and anonymity were identified as factors influencing misuse by Zhang, Oh and Teo (2006), however current research did not provide evidence to support the previous findings. This may have been due to the environment of the experiment. When an employee is asked whether he/she would engage in non-work related activities provided that they are anonymous, having the prior knowledge and understanding of internet access through a proxy server (where each and every request is being recorded) one may tend to answer negatively. It can not be concluded that this was the exact reason for this observation but it may have had an influence on the results. Further authors observed a negative correlation (correlational coefficient – 0.611) between the level of awareness of acceptable use policy and the level of misuse suggesting that the awareness reduces misuse.

5.4 Results

80% of large scale organizations possessed some form of a written guideline while only 18.18% of medium scale organizations possessed the same.

The null hypothesis H_0, that is: 'Acceptable Use Policy does not make a difference in employee computer misuse' was accepted at 5% level.

Not having access to Internet/email out side the work place makes employees engage in more misuse.

Organizational structure is a significant influence on employee computer misuse.

6. CONCLUSION

According to the findings of this research the following conclusions were made. The existence of an Acceptable Use Policy in a Software Organization does not make a significant difference in employee computer misuse. Having internet, email access only at work is a significant factor that influences work computer misuse. Organizations with high centralized decision making, narrow span of control and high level of formalization enjoy significantly low levels of employee computer misuse. Peer influence does have an effect on employee computer misuse.

7. LIMITATIONS

Any inference on employee computer misuse of employees of small scale software development organizations or employees of software development organizations in general cannot be made using this research as it focused only the employees of large and medium scale software development organizations.

The sample size of this research was 88 which falls below the minimum sample size required to produce 95% confidence in findings (Sekaran 2006, p. 294). Therefore in generalizing the confidence levels of findings need to be taken into account.

The research design was a one-time survey that produced a profile of each employee's usage behavior of work computers. This type of cross-sectional design precludes being able to draw any conclusions about cause and effect relationships between these characteristics. Since the study is only co relational and hypothesis testing one time survey can be justified.

Random sampling was used in selecting samples from the organizations participated. This type of selection of respondents can be expected to produce samples that are reasonably representative of the employees of different sub-groups (sub- groups here are different organizations). However, non responsiveness observed from some of the organizations may serve to bias the sample in ways that are not readily evident.

8. FUTURE RESEARCH

This study can be considered a starting point for research on Acceptable Use Policies in Sri Lanka. The future research can concentrate on other industries in determining whether the acceptable use policies are effective. Experimental studies on the level of exposure to use policies needed to build awareness can be studied to identify the optimum level of exposure required to give adequate level of awareness to the employees. Further the most influential mode for awareness building can be studied as an experimental research where different methods of exposure to acceptable use policies would be provided for different groups and awareness building would be studied in each of the groups.

Future research can also focus on policy enforcement levels and the effectiveness of the policy. Monitoring levels of policy adherence, penalties for non adherence and how they influence the effectiveness of policy can also be an interesting area of study.

REFERENCES

Asian Development Bank (2001) Report and Recommendation of President to the Board of Directors on Proposed Loan, Partial Credit Guarantee and Technical Assistance to Democratic Socialist Republic of Sri Lanka for the SME Sector Development Program, RRP: SRI 33246, accessed on 10-08-2007, <http://www.adb.org/Documents/RRPS/SRI/rrp_33246.pdf>

Case, C. J. and Young, K. S. (2001) Internet Risk Management: Building a Framework for Research, *Proceedings of the American Society of Business and Behavioral Sciences*: 16-18.

Case, C. J. and Young, K. S. (2002) Employee Internet Use Policy: An Examination of Perceived Effectiveness, accessed on 11-03-2007, <http://www.iacis.org/iis/2002_iis/PDF%20Files/CaseYoung.pdf>

Chang, S. E. and Lin, C. S. (2007) Exploring Organizational Culture for Information Security Management, *Industrial Management & Data Systems* 107(3): 438-48.

Department of Censes and Statistics – Sri Lanka (2004) Computer Literacy of Sri Lanka, accessed on 26-08-2007, <http://www.statistics.gov.lk/cls2004/index.htm>

Dhillon, G. (1999) Managing and Controlling Computer Misuse, *Information Management & Computer Security* 7(4): 171-175.

Enbysk, M n.d, Should You Monitor Your Employee's Web Use?, accessed on 22-02-2007, <http://www.microsoft.com/smallbusiness/resources/management/employee-relations/should-you-monitor-your-employees-web-use.mspx>

Foltz, C. B, Cronan, T. P. and Jones, T. W. (2005) Have You Met Your Organization's Computer Usage Policy?, *Industrial Management & Data Systems* 105(2): 137-146.

Gattiker, E. and Kelley, H. (1999) Morality and Computers: Attitudes and Differences in Judgments, *Information Systems Research* 10(3): 233-254.

Harrington, S. J. (1996) The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions, *MIS Quarterly*, 20(3): 257-278.

Information and Communication Technology Agency of Sri Lanka (2005) Information Systems Acceptable Use, accessed on 08-10-2007, <http://www.icta.lk/Insidepages/ReGov/ICTPolicy/ICTPolicyDocs/12-Information%20Systems%20Acceptable %20Use.pdf>

Kanungo, S. (1998) An Empirical Study of Organizational Culture and Network-Based Computer Use, *Computer in Human Behavior* 14(1): 79-91.

Kreie, J. and Cronan, T. P. (1998) How Men and Women View Ethics, *Communications of the ACM* 31(9): 70-76.

Kapurubandara, M. and Lawson, R. (2006) Barriers to ICT and e-commerce with SMEs in Developing Countries: An Exploratory study in Sri Lanka, accessed on 10-08-2007, <http://www.collecter2006.unisa.edu.au/Paper%209%20Mahesha%20Kapurubandara.pdf >

Lawrence, P. (n.d.) Acceptable Use: Whose Responsibility is it?, accessed on 12-02-2007, <http://www.attackprevention.com/article/Acceptable_Use_Whose_ Responsibility_ Is_It-792.html>

Leonard, L. N. K. and Cronan, T. P. (2005) Attitude toward Ethical Behavior in Computer Use, *Industrial Management & Data Systems* 105(9): 1150 – 1171.

Lichtenstein, S. and Swatman, P. M. C. (1997) Internet Acceptable Usage Policy for Organizations, *Information Management and Computer Security* 5(2): 182-190.

Marson, C. D. (2000) Are workers cyber-moonlighting? accessed 18-03-2007, <http://archives.cnn.com/2000/TECH/computing/03/08/moonlight.idg/index .html>

Mastrangelo, P. M. , Everton, W. and Jolton, J. A. (2006) Personal Use of Work Computers: Distraction versus Destruction, *Cyber Psychology & Behavior* 9(6): 730 – 741.

McShane, S. L. and Glinow, M. A. V. (2005) *Organizational Behavior*, 3rd edition, Tata McGraw-Hill, New Delhi.

Peterson, D. K. (2002) Computer Ethics: The Influence of Guidelines and Universal Moral Beliefs, *Information Technology & People* 15(4): 346 - 361.

Pierce, M. A. and Henry, J. W. (1996) Computer Ethics: The Role of Personal, Informal and Formal Codes, *Journal of Business Ethics* 15(4): 425- 437.

Pierce, M. A. and Henry, J. W. (2000) Judgements about Computer Ethics: Do Individual, Co-worker, and Company Judgements Differ? Do Company Codes Make a Difference, *Journal of Business Ethics* 28(4): 307 – 322.

Schulman, A. (2001) The Extent of Systematic Monitoring of Employee Email and Internet Use, accessed on 10-03-2007, <http://www.diogenesllc.com/internetmonitoring.pdf>

Sekaran, U. (2006) *Research Methods for Business A Skill-Building Approach*, 4th edition, John Wiley & Sons (Asia), Singapore.

Sri Lanka Information and Communication Technology Association (2007) Rising Demand: The increasing demand for IT workers spells a challenging opportunity for the IT industry, accessed on 03-09-2007, <http://www.icta.lk/Insidepages/downloadDocs/ICTWorkforcSurvey2007. pdf>

Sri Lanka Telecom Official Site (n.d) SLTNET Internet Prepaid Card (IPC), accessed on 09-10-2007, <http://www.slt.lk/data/forhome/093sltnet_prepaid.htm>

Stephan, B. and Petropoulakis, L. (2007) The Design and Implementation of an Agent-based Framework for Acceptable Usage Policy Monitoring and Enforcement, *Journal of Network and Computer Applications* 30(2): 445-465.

Totten, J. A. (2004) The Misuse of Employer Technology by Employees to Commit Criminal Acts, *Proceedings of the ABA Section of Labor and Employment Law Technology Committee Midyear Meeting*, Labor and Employment Law Technology Committee, Miami.

Verespej, M. A. (2000) Inappropriate Internet Surfing, Industry Week, 02 July 02, accessed on 10-03-2007, <http://www.industryweek.com/CurrentArticles/asp/ articles.asp?ArticleId=740>

Vitell, S. J. and Davis, D. L. (1990) Ethical Beliefs of MIS Professionals: The Frequency and Opportunity for Unethical Behavior, *Journal of Business Ethics* 9: 63 – 70.

Walsham, G. (1996) Ethical Theory, Codes of Ethics and IS Practice, *Information Systems Journal* 6: 69 – 81.

WeComply Inc. (2007) Nothing Personal: Survey of Computer Use at Work, accessed on 11-03-2007, <http://www.wecomply.com/media/Nothing_Personal_Report.pdf>

Wheelen, T. L., Hunger, J. D. and Rangarajan, K. (2006) *Concepts in Strategic Management and Business Policy*, 9th edition, Korling Kindersley Pvt. Ltd., Delhi.

Zetter, K. (2007) Is Your Boss Spying on You? It's legal, it's happening and it can get you fired, *Reader's Digest* - November, 97 - 103.

Zhang, D. , Oh, L. B. & Teo, H. H. (2006) An Experimental Study of the Factors Influencing Non-Work Related Use of IT Resources at Workplace, *Proceedings of the thirty ninth Hawaii International Conference on System Sciences:* 206a.

APPENDIX – A

Table 2: Sample Demographic - Gender

	No of Respondents	Percentage
Male	60	68.2
Female	28	31.8

Table 3: Sample Demographic - Education

Qualification	No of Respondents	Percentage
A/L	3	3.4
Graduate–Private University	31	35.2
Graduate – State University	39	44.4
Postgraduate	15	17.0

APPENDIX – B

1. I use my office email to send personal messages
   I use my office email to send forward jokes/ humorous materials/chain mails to friends
2. I am using internet access at work to find information for my personal interest
3. I have downloaded music/pictures/software using office internet connection
4. I have done at least one of the following using my office internet access. Personal banking transactions/ channeling doctors/ paying bills/ online shopping/ chatting with friends
5. I have installed software in my office computer (which was not given by the office) for my personal use
6. I am using my office computer to do my personal work like typing letters, writing CDs etc.
7. I have played games using my office computer
8. I share my office computer's password with my colleagues