IADIS International Journal on Computer Science and Information Systems
Vol. 7, No. 2, pp. 87-100
ISSN: 1646-3692

A MANAGERIAL INCENTIVE FOR WORKPLACE ELECTRONIC SURVEILLANCE

Viraj Samaranayake. *Department of Computer Science and Engineering - University of Moratuwa-Moratuwa, 10400, Sri Lanka.*

Chandana Gamage. *Department of Computer Science and Engineering - University of Moratuwa-Moratuwa, 10400, Sri Lanka.*

ABSTRACT

Electronic monitoring at workplace is a rapidly growing phenomenon in the modern world. It allows employers to observe what employees do on the job and review employee communications, including e-mail and internet activity that employees consider private. In a survey done among the software development organizations in Sri Lanka, it was found that majority of the companies use some means of electronic technology to monitor their employees. Most of the time, employee perception towards electronic monitoring at work, contradicts with the need for law enforcement within the organization as intended by the top management. Employers justify electronic monitoring at workplace in terms of protecting the company's confidential information, preventing the misuse of the organizational resources while uplifting the quality of work and productivity. On the other hand, the mutual trust that should be there between the employer and the employee is brought into question by such monitoring. The research results presented in this paper are based on a study that investigated electronic monitoring in multiple perspectives from the view point of software professionals in Sri Lanka. The study focused on analyzing managerial incentives for electronic monitoring at workplace, to find how it could significantly influence organizational IT security policy making.

The research was based on an empirical study with a structured questionnaire, utilizing disproportionate stratified random sampling. The research study collected data on important issues such as Perceived Level of Infringement, Perceived Relevance to Work, Perceived Invasion of Privacy and Personal Judgment of Effectiveness of the software professionals, in Sri Lanka. The research found that if electronic monitoring is intended for a valid purpose, it is generally accepted by the software professionals. Majority of the subjects responded against electronic monitoring if it invades their privacy. However, they accepted electronic monitoring to a certain extent if it monitors only the tasks associated with the job. Further the respondents did not object to having electronic monitoring at workplace if it is to ensure their quality of work. The findings of this research can be incorporated in IT security policy making in the software development organizations in Sri Lanka and in similar economics with large scale offshore software development enterprises, with a special emphasis on the employees, which is the most valuable asset of the organization.

KEYWORDS

Electronic monitoring, Software professionals, Relevance to work, Personal judgment of effectiveness, Invasion of privacy

1. INTRODUCTION

1.1 Electronic Monitoring

Electronic monitoring refers to the use of computerized systems to automatically collect, store, analyze, and report information on employee activities at work. It is a device or system that allows an employer to observe what employees do on the job and review employee communications, including e-mail and internet activity, often capturing and reviewing communications that employees consider private.

Electronic monitoring makes it possible to monitor many employees simultaneously and to obtain much more detailed information at the same time. According to Flanagan (1994), electronic monitoring makes it possible for the employers to monitor the activities of their employees continuously and secretly. Further he explains that if an employee's workplace is equipped with a full-featured computer network, a manager can eavesdrop on all components of the employee's computer work without the employee's consent.

Today, almost all jobs have the potential to be subjected to electronic monitoring. As part of the pilot study carried out for the current research, preliminary interviews were conducted for randomly selected software professionals and top level managers representing major software organizations in Sri Lanka. This enabled the researchers to gain some understanding about the nature of the electronic monitoring mechanisms installed at organizational level along with their perceived consequences from different viewpoints. According to the information gathered, it was evident that the majority of the software development organizations in Sri Lanka today use some means of electronic technology to monitor their employees' activities. There are cases reported in Sri Lanka recently of job termination of software professionals, due to the conflicts of interest aroused among the employee and the employer as a result of the electronic monitoring at workplace. Most of the software professionals perceive this as a serious matter because the mutual trust that should be there between the employer and the employee is in question. A probable outcome would be the unhappiness and dissatisfaction at work. No significant research has been carried out within the context of Sri Lanka, focused on analyzing managerial incentives for electronic monitoring at workplace to find out how it could significantly influence organizational IT security policy making.

However this seems to be a topic of great research interest internationally such that several studies and surveys are carried out to find out the impact of electronic monitoring within the organizational context. According to the Electronic Monitoring and Surveillance Survey 2007, released by the American Management Association (2007), which was carried out among 304 organizations in the United States, more than one fourth of the employers fired workers for misusing e-mail and nearly one third have fired employees for misusing the internet. Two thirds of employers monitored the internet connections because, they are primarily concerned about inappropriate web surfing. High percentages (65%) of companies use software to block connections to inappropriate websites, which is a 27% increase since the first survey conducted in 2001.

Without e-mail systems and internet, it is very difficult to run a business today. However, day by day as electronic business activity increases, ad-hoc email implementation, prolonged management neglect and user abuse of email systems have generated negative effects. As an employer it is very hard to foresee, control and prevent these negative effects. Many employers try to control the negative effects of email through a combination of policies and electronic monitoring. Wen et al. (2007) stated that the employee access to surf and browse is subjected to monitoring via reports, active daily monitoring and on-line notification. Therefore the technology is capable of taking pictures of an employee’s screen at periodic intervals, which enables the employer to see the sites employees are visiting, the messages they are e-mailing, and the confidential information they may possibly be exposing. This indicates that it is not only the employees’ internet usage that is being monitored, but also the screen content of their e-mail, for potentially offensive or inappropriate messages. They investigated about software solutions that help employers to monitor employees’ machines and/or send e-mail reports to a specified e-mail address. Some of the applications send exact copies of employees’ e-mails, chats, instant messages, and usage of sensitive words and phrases to a specified e-mail address instantaneously.

Most employers have good business justifications to electronically monitor employees in the workplace including assessing worker productivity, protecting company assets from misappropriation, and ensuring compliance with workplace policies. In the worst case scenarios, some internet abuse problems, including pornography, gambling, online auctions, chat rooms and blogging, can create corporate liability with illegal activities and potential lawsuits.

1.2 Research Objectives

This study has been carried out to investigate electronic monitoring in multiple perspectives from the view point of software professionals in Sri Lanka, to analyze managerial incentives for electronic monitoring at workplace and to find how it could significantly influence organizational IT security policy making. Based on insights gained from this study, employers can take proactive actions to make IT security policies by considering the views of their employees.

2. RELATED WORK

The impact of electronic monitoring at workplace and finding out relationships on how it could significantly influence organizational IT security policy making is an interesting area of study in the field of software industry. Since the human factor is involved, previous research has been influenced heavily by employer side to find out the relationship between electronic performance monitoring and employee behavior. With the evolvement of the area of research, many researchers contributed to the knowledge by comparing various areas with respect to electronic monitoring.

Electronic monitoring refers to the use of electronic hardware and software to collect, analyze, and report individual or group actions or performance (Alder and Ambrose, 2005).

The definition of electronic monitoring, or electronic task-specific monitoring (Stanton, 2000) in the workplace varied in past research as technological advances caused monitoring practices to increase in complexity and prevalence. Internet and email allow employees to communicate effectively and efficiently with others. On the other hand, employers use tools to monitor employees in the workplace. This monitoring could help to reduce employees' misconduct, increase productivity and prevent leakage of confidential information (Samantha and Kleiner, 2003).

As long as there has been employment, employees have been monitored (Nebeker and Tatum, 1993). The Electronic Monitoring and Surveillance Survey 2007, released by the American Management Association (2007), suggest that the most frequently occurring electronic monitoring techniques include the monitoring of computer files, computer output including e-mail and internet activity, telephone calls, and video camera surveillance to directly observe employee behaviors. While almost all jobs have potential to be subjected to some type of electronic monitoring, some are much more susceptible to this activity. Alder and Ambrose (2005) state that the organizations utilizing electronic monitoring procedures must also decide the extent to which performance information will be provided to employees. However, in recent years, with an environment of affordable technology, the availability of less easily observable or detectable monitoring devices, and a lack of adequate regulation, there has been an explosion in the use of electronic monitoring and surveillance in the workplace. During the past two decades, workplace surveillance has been steadily on the rise (Aiello, 1993; Aiello and Svec, 1993; Vorvoreanu and Botan, 2000) and its frequency is still increasing.

Employers have the right to monitor employees in the workplace during working hours because they are responsible for all of the activities, including the company's information and employees' safety, which happen during the working hours. On the other hand, employees have the right to privacy under common law. Therefore, employers must define clear and understandable policies about electronic monitoring of employees in the workplace. Moreover, employers need to clearly define to what extent they intend to monitor the workplace (Samantha and Kleiner, 2003).

According to Ariss (2002), the workplace monitoring is considered as an important control measure for business necessity for the following reasons.

- Workplace monitoring may prevent the misuse of the organizational resources and the related expenses incurred
- Workplace monitoring may enhance the company security in terms of business secrets, intellectual assets, and corporate knowledge
- Monitoring may lead to the avoidance of legal liabilities resulted from employee misbehaviors
- Monitoring may increase the employee performance

In Sri Lanka, legislative work on a data protection act incorporating privacy laws has progressed towards enaction (Mahanamahewa, 2007). This establishes guidelines for Sri Lankan employers on minimum standards for privacy protection. Balancing the legitimate need of employers to monitor the workplace with respect for individual privacy is not difficult. The best course of action is to have a monitoring policy and follow it (Wakefield, 2004).

According to Meyers (2003), over the past decade, the realm of technology and privacy has been transferred, creating a landscape that presents new challenges for employees. They studied the actual relationships between monitoring, surveillance and their impacts on employees' privacy needs and attendant control belief need. Wakefield (2004) asserts that, for an employer, it is recommended that organizations have a written policy clearly stating that any right to privacy is waived for documents and messages created, stored, sent or received on the organization’s computer systems or over its networks. He further states that the clear-cut policies set boundaries, establish employees’ expectations of privacy, and help set a workplace tone that conveys organizational responsibility and respect for others.

According to American Management Association (2007), employers cannot expect an uninformed workforce to comply with policy. And they cannot trust employees on their own to access the company intranet system or retrieve a copy of the employee handbook in order to educate themselves about monitoring or other electronic rules and policies. Employer should introduce policies and the best practices call for formal employee training, which grant employees the opportunity to ask questions and gain a thorough understanding of electronic rules, policies, and procedures.

According to the study carried out by Ariss (2002), there are some recommendations for electronic monitoring for employers.

- Identify the business purpose for the monitoring and confine it to what is necessary to accomplish that purpose. Monitoring will only be used as necessary and will not be intrusive on the employees’ computer work
- Require every employee to sign a statement that authorizes organization to monitor e-mail and computer usage. This statement makes it clear that employees should have no expectations of privacy in their electronic communications
- Develop and provide employees a written policy on employee use of communication systems, outlining exactly what types of communication are prohibited.
- Inform all employees how and when they will or might be monitored and what standards will be used to evaluate their performance
- Inform employees that employee passwords for company systems do not guarantee privacy and may be overridden. Require employees to notify an administrator of their passwords to further decrease their expectation of privacy

Wakefield (2004) identified several major aspects to maintain the minimum, comprehensive monitoring policy. He suggested that below basic policies should be included in the electronic monitoring policy for every organization.

- State the specific business purposes for monitoring
- Clearly state the ownership of company computers, networks, files and e-mail
- Clearly outline the forms of communication considered illegal, prohibited and unacceptable
- Clearly outline the web sites considered illegal, prohibited and unacceptable
- Define the acceptable use of company networks and e-mail
- Set clear boundaries for the personal use of company networks
- Inform employees of the specific types of monitoring activities that will be used
- Explain how monitoring activities are advantageous to employees, clients and the company
- Determine the consequences for policy violations

3. METHODOLGY

3.1 Research Method

This study investigated electronic monitoring in multiple perspectives from the view point of software professionals in Sri Lanka. Perceived Level of Infringement, Perceived Relevance to Work, Perceived Invasion of Privacy and Personal Judgment of Effectiveness were specifically considered.

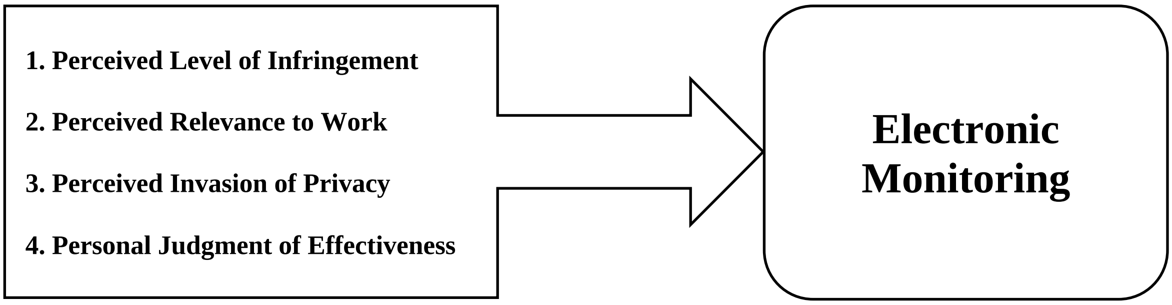
1. Perceived Level of Infringement
2. Perceived Relevance to Work
3. Perceived Invasion of Privacy
4. Personal Judgment of Effectiveness
Electronic Monitoring

Figure 1. Multiple perspectives of electronic monitoring.

Perceived Level of Infringement means whether electronic monitoring is viewed as something which intrudes into one's work. Perceived Relevance to Work means whether electronic monitoring is viewed as something relevant to the work. Perceived Invasion of Privacy means whether electronic monitoring is viewed as something which violates the employees' privacy at work. Personal Judgment of effectiveness refers to the personal judgment of the software professional regarding the effectiveness of electronic monitoring at workplace. The multiple perspectives in electronic monitoring are illustrated in Figure 1.

3.2 Method of Data Collection and Sampling

The target population for this research was the software professionals working in software organizations as well as non-software organizations such as in-house software development companies in Sri Lanka, covering both private sector and government sector organization.

Information Communication Technology Agency (2007) workforce survey was used to assess the population size and it was estimated to be 33,048. Using the formula used by Krejcie and Morgan (1970), sample size for this study was estimated to be 380, at the confidence interval of 0.05 and confidence level of 95%. Disproportionate stratified random sampling was used on the basis of the professional experience of the software professionals. 209 from less than 5 years level, 116 from 5 – 10 years level, 45 from 11 – 15 years level and 10 from above 15 years level of professional experience were estimated.

Based on the background survey results along with the essence of previous research, a questionnaire instrument was constructed with 10 questions in five point Likert scale to measure the variables. Initially, a pilot study was carried out to ensure the reliability of the questionnaire. Once the reliability was validated, the questionnaire was made available online for the target respondents. Statistical analysis was carried out to find out the outcome of this research.

4. DATA ANALYSIS AND DISCUSSION

Both reliability analysis and descriptive statistical analysis were carried out based on the feedback received from the questionnaire. In order to measure Perceived Level of Infringement, Perceived Relevance to Work, Perceived Invasion of Privacy and Personal Judgment of Effectiveness, 2, 2, 4 and 2 questions were used respectively. For this purpose, a five-point Likert scale ranging from Strongly Disagree (valued as a "1") to Strongly Agree (valued as a "5"), was used. In addition, five demographic items were used to capture the respondent's age, gender, education level, nature of organization (Private sector/ Government Sector) and nature of the tasks assigned in the organization.

Before carrying out any analysis on the data, reliability analysis was conducted to check the goodness of the instruments. To check the reliability of the questionnaire, a pilot survey was carried out for 40 respondents and the Cronbach's Alpha Coefficient was calculated. All the variables had acceptable reliabilities without eliminating any of the items with above 0.7 values for Cronbach's Alpha Coefficient. Finally, the reliability test was carried out for the research survey for the entire sample of 380 respondents and all variables passed the reliability test with above 0.7 values for Cronbach's Alpha Coefficient.

The sample contained 302 (79.47%) males and 78 (20.53%) females. Considering the age distribution, 210 (55.26%) were between 20 -30 years, 158 (41.58%) were between 31- 40 years, 12 (3.16%) were between 41-50 years and no respondent was there from the age group of above 50 years. In Sri Lanka, it seems difficult to find software professionals from the age group of above 50 years. 285 (75.00%) had Graduate Degrees, 73 (19.21%) had Post Graduate Degrees, 22 (5.79%) had Diploma and there were no respondents who are only High School certified. Every software professional had at least been certified in a computer related Diploma.

In this survey, all software development organizations in Sri Lanka were categorized based on the number of employees. The groups were: less than 50 employees, 50 - 100 employees, 100 – 500 employees, 500 – 1000 employees and above 1000 employees. 82 were reported from less than 50 employees category, 9 were reported from 50 - 100 employees category, 175 were reported from 100 – 500 employees category, 15 were reported from 500 – 1000 employees category and 99 were reported from above 1000 employees category. There were 368 respondents from Private sector organizations and 12 respondents from Government sector organizations. In Sri Lanka, software professionals in the government sector organizations are rather less.

The sample contained 209 (55%) professionals of less than 5 years' of professional experience in the software industry, 116 (30.53%) of between 5 - 10 years' professional experience in software industry, 45 (11.84%) of between 10 - 15 years' professional experience in software industry and 10 (2.63%) of above 15 years' professional experience in software industry.

Table 1 presents the summary information for the first questionnaire item of Perceived Level of Infringement. Responses were more towards Agree or Strongly Agree side and it was 73.9%. This means 281 respondents of the software professionals responded against electronic monitoring which is used in their organizations to monitor employee activities. Table 2 presents the summary information for the second questionnaire item of Perceived Level of Infringement. It seems that 92.1% of the software professionals feel uncomfortable to think that somebody in their organization is always watching their activities at work. Also the Mean of the responses for item 2 is 4.50.

Table 1. Perceived Level of Infringement – Item No. 1

My work being monitored by my employer is unacceptable because, it is something like intruding into one’s work				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1(Strongly Disagree)	4	1.1	1.1	1.1
2(Disagree)	60	15.8	15.8	16.8
3(Neither Agree nor Disagree)	35	9.2	9.2	26.1
4(Agree)	138	36.3	36.3	62.4
5(Strongly Agree)	143	37.6	37.6	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
3.94	1.093	1.1	1	5

Table 3 and 4 present the survey summary results for Perceived Relevance to Work questionnaire items. The responses were more towards Disagree or Strongly Disagree side for both questions. Based on the results, it seems that most of the software professionals have a good awareness about electronic monitoring and how it is related to their work. Considering the item 1, 61.3% indicated that they understand the connection between their work and electronic monitoring at their workplace. According to item 2, 69.2% understand the role of electronic monitoring in the computer activities related to their work. However, outcome of the both items shows that, almost 20% lack understanding about the connection between electronic monitoring and how its related to their work. This indicates that a significant number of Sri Lankan software development organizations do not officially inform their employees about the role of electronic monitoring in their organization or else these employees are not very concerned about electronic monitoring and its importance in the workplace.

Table 2. Perceived Level of Infringement – Item No. 2

I would feel uncomfortable to think that somebody in my organization is always watching my activities at work				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	2	.5	.5	.5
2	21	5.5	5.5	6.1
3	7	1.8	1.8	7.9
4	104	27.4	27.4	35.3
5	246	64.7	64.7	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
4.50	.827	.683	1	5

Table 3. Perceived Relevance to Work – Item No. 1

I cannot understand the connection between my work and electronic monitoring going on at my workplace				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	53	13.9	13.9	13.9
2	180	47.4	47.4	61.3
3	72	18.9	18.9	80.3
4	72	18.9	18.9	99.2
5	3	.8	.8	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
2.45	.978	.956	1	5

Table 4. Perceived Relevance to Work – Item No. 2

I cannot understand what electronic monitoring has to do with the computer activities related to my work				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	123	32.4	32.4	32.4
2	140	36.8	36.8	69.2
3	33	8.7	8.7	77.9
4	82	21.6	21.6	99.5
5	2	.5	.5	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
2.21	1.131	1.280	1	5

Table 5 presents the summary information for the questionnaire item 1 of Perceived Invasion of Privacy. 81% of the software professionals did indicate concern about their privacy, regardless of the fact that they are paid for their work. Therefore, they do not accept electronic monitoring if their privacy is being violated. This emphasizes the importance of introducing standard policies associated with electronic monitoring and sharing these with the employees prior to establishing them. It is worthwhile to provide the employees with the opportunity to ask questions and incorporate their feedback in preparing the said policies.

Table 5. Perceived Invasion of Privacy – Item No. 1

Even though we are paid for our work, we are entitled to a certain degree of privacy, and should not be monitored by computers and other electronic devices by the employer				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	3	.8	.8	.8
2	50	13.2	13.2	13.9
3	19	5	5	18.9
4	149	39.2	39.2	58.2
5	159	41.8	41.8	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
4.08	1.030	1.062	1	5

According to the summary of the results for questionnaire item 2 of Perceived Invasion of Privacy, 84.5% (Table 6) of the software professionals do not have any objection towards implementing a workplace privacy policy. However, they do not believe in monitoring everything at workplace. Again, this shows that it is always better to incorporate employee feedback in implementing workplace IT security policy and also communicate it down to the employees. Otherwise, there will be a conflict between employer and employees.

Table 7 and 8 present summary of the responses received for Perceived Invasion of Privacy. According to the results, majority of the software professionals' general perception is such that the electronic monitoring at workplace is unfair and unethical. Further, most of them are of the view that their privacy in the hands of the employer might pose a threat to their physical and mental health. This emphasizes the importance of having an organizational IT security policy which clearly states that any right to employee privacy is waived off for documents and messages created, stored, sent or received on the organization's computer systems or over its networks.

Table 6. Perceived Invasion of Privacy – Item No. 2

I do not feel any conflict about implementing a workplace privacy policy, but I believe that all should not be monitored electronically				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	2	.5	.5	.5
2	37	9.7	9.7	10.3
3	20	5.3	5.3	15.5
4	155	40.8	40.8	56.3
5	166	43.7	43.7	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
4.17	.948	.899	1	5

Table 7. Perceived Invasion of Privacy – Item No. 3

I feel that electronic monitoring is unfair and unethical				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	2	.5	.5	.5
2	54	14.2	14.2	14.7
3	39	10.3	10.3	25.0
4	106	27.9	27.9	52.9
5	179	47.1	47.1	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
4.07	1.090	1.188	1	5

Table 8. Perceived Invasion of Privacy – Item No. 4

I am objecting to electronic monitoring because my privacy in the hands of my employer might pose a threat to my physical and mental health				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	2	.5	.5	.5
2	49	12.9	12.9	13.4
3	35	9.2	9.2	22.6
4	75	19.7	19.7	42.4
5	219	57.6	57.6	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
4.21	1.091	1.190	1	5

Considering all the items used to measure Perceived Invasion of Privacy, it seems that for every item, over 75% of the respondents indicated that they are in fact concerned about their privacy. Item Means ranged from 4.07 to 4.21. Therefore, the majority of the software professionals responded against electronic monitoring at work which might violate their privacy. On the other hand they were less concerned about electronic monitoring if it does not monitor everything at work.

According to Wakefield (2004), it is not easy to maintain the balance between the employer and employee, without having a reasonable monitoring policy that also meets individual privacy expectations. The research findings of the present study also assert the importance of having a privacy policy in software organizations.

Table 9 and 10 present the summary of the responses received for the measures of Personal Judgment of Effectiveness. 89% (Table 9) of the respondents accepted electronic monitoring of their activities if it is to ensure their quality of work. This is an important fact that software development organizations need to consider when implementing electronic monitoring at the workplace. Overall, the results indicate that electronic monitoring can be promoted effectively emphasizing the importance of ensuring the organizational goals such as improving the work quality.

Table 9. Personal Judgment of Effectiveness – Item No. 1

I think it is acceptable that the employer has an interest in monitoring employee activities to ensure quality of work				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	2	.5	.5	.5
2	9	2.4	2.4	2.9
3	31	8.2	8.2	11.1
4	213	56.1	56.1	67.1
5	125	32.9	32.9	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
4.18	.721	.520	1	5

Table 10. Personal Judgment of Effectiveness – Item No. 2

I think it is acceptable for the employer to electronically monitor the employees, if they really don't trust their employees				
Scale	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	1	.3	.3	.3
2	15	3.9	3.9	4.2
3	87	22.9	22.9	27.1
4	81	21.3	21.3	48.4
5	196	51.6	51.6	100.0
Total	380	100.0	100.0	
Mean	**Std. Deviation**	**Variance**	**Min.**	**Max.**
4.20	.943	.899	1	5

In the present study, disproportionate stratified random sampling method was used, on the basis of the professional experience of software professionals in Sri Lanka. The 4 stratums were: less than 5 yrs, 5 - 10 yrs, 10 -15 yrs and above 15 yrs. In order to evaluate the effect of professional experience on electronic monitoring, one-way ANOVA test was carried out for each variable at the 0.05 confidence interval.

Table 11. Electronic Monitoring and Professional Experience of Software Professionals

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.987	3	.662	2.707	.045
Within Groups	92.006	376	.245		
Total	93.993	379			

As illustrated in Table 11, the F value of 2.707 is significant at the .045 level. This implies that, along with high professional experience, there is a relationship between professional experience of software professional and electronic monitoring.

5. CONCLUSION

Based on the research findings, Electronic Monitoring can be seen as a form of discipline. As such, the possibility that electronic monitoring will be met by resistance in the workplace should come as no surprise. In fact, some of the negative effects of electronic monitoring discussed under invasion of privacy can best be interpreted as acts of resistance. The experience of being monitored acquires meaning as it is lived and interpreted by people in their organizational contexts. Depending on the nature of this social construction, electronic monitoring can be perceived as a more or less negative experience, and can have varying effects. Therefore, electronic monitoring as a form of discipline and resistance as a form of anti-discipline may differ from one social context to another and even from one individual to another, depending on various influences. It is important to note that the software professionals accept implementing workplace IT security policy, but they believe that all should not be monitored electronically. Also the software professionals are less concerned about electronic monitoring if it is to ensure the quality of their work. Therefore, managements of the software organizations should make sure that the electronic monitoring activities are conducted in the intention of uplifting the work quality and productivity. The negative attitudes towards electronic monitoring could be effectively reduced if these two aspects are taken into consideration in electronic monitoring IT security policy making.

ACKNOWLEDGEMENT

The support given by the staff of the MBA in IT program of University of Moratuwa, Sri Lanka, and by the software professionals in Sri Lanka, is gratefully acknowledged.

REFERENCES

Flanagan, J.A., 1994. Restricting Electronic Monitoring in the Private Workplace. *Duke Law Journal*, Vol. 43, No. 6, Twenty- Fifth Annual Administrative Law Issue, pp. 1256-1281.

American Management Association, 2007. The Latest on Workplace Monitoring and Surveillance. [Available at]: http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/. [Accessed]: 10 –MAY-2010

Wen, J.H., et al, 2007. Internet Usage Monitoring in the Workplace- Its Legal Challenges and Implementation Strategies. *Information Systems Management*, Vol. 24, pp. 185–196.

Alder, G. S., and Ambrose, M. L., 2005. Towards understanding fairness judgments associated with computer task specific monitoring: An integration of the feedback, justice, and monitoring research. *Human Resource Management Review*, Vol. 15, pp. 43-67.

Stanton, J.M., “Reactions to employee task-specific monitoring: Framework, review, and research directions,” *Human Performance*, 2000, Vol. 13, No. 1,pp. 85-113, In A.W. Watson, “Electronic Monitoring Relevance And Justification: Implications For Procedural Justice And Satisfaction,” *Thesis*, North Carolina State University, 2007.

Samantha, L., and Kleiner, B.H., 2003. Electronic Surveillance In The Workplace. *Journal of Management Research News*, Vol. 26, pp. 72-81.

Nebeker, D.M., and Tatum, B.C., 1993. The effects of computer monitoring, standards and rewards on work performance, job satisfaction, and stress. *Journal of Applied Social Psychology*, Vol. 23, No. 7, pp. 508-536.

Vorvoreanu, M. and Baton, C.H., 2000. Examining Electronic Surveillance In The Workplace: A Review Of Theoretical Perspectives And Research Findings, Paper From *Conference Of The International Communication Association*. Mexico, Acapulco, pp. 3.

Aiello, J.R., 1993. Computer-Based Work Monitoring: Electronic Surveillance and Its Effects. *Journal of Applied Social Psychology*, Vol. 23, No. 7, pp. 499-507.

Aiello, J.R., and Svec, C.M., 1993. Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence. *Journal of Applied Social Psychology*, Vol. 23, No. 7, pp. 537-548.

Ariss, S.S., 2002. Computer Monitoring: Benefits and Pitfalls Facing Management. *Information & Management*, Vol. 39, No. 7, pp. 553–558.

Mahanamahewa, P., PHR2006 - Republic of Sri Lanka. Privacy International. Retrieved on: Aug 20, 2011, Located at: https://www.privacyinternational.org/article/phr2006-republic-sri-lanka, 2007.

Wakefield, R.L., 2004. Employee Monitoring and Surveillance: The Growing Trend. *Information Systems Control Journal*, Vol. 1, pp. 47-49.

Meyers, N., 2003. Employee Privacy In The Electronic Workplace: Current Issues For It Professionals. *14th Australasian Conference on Information Systems*. Western Australia, Perth.

Information Communication Technology Agency, 2007. Sri Lanka IT Workforce Survey, [Available at]: http://www.slicta.lk/news/fullreport/ict%20wfsr2007.pdf , [Accessed]: 19 –JAN-2010.

Krejcie, R.V., and Morgan, D.W., 1970. Determining Sample Size For Research Activities, *Educational And Psychological Measurement*, Vol. 30, pp. 607-610.