Security and privacy in workplace

1. 0 Introduction Whalen and Gates (2010), define monitoring differently in their article. They define it as a method and procedure of examining the workers in an organization and study their constant events intended to guarantee that together the protection of employees and requirements of the employer are met. Nearly all companies nowadays take videos of their employees, they read their emails and monitor their Web surfing. This can be done surreptitiously and some organizations are honest about it Chan et al. (2005). Privacy is one of the most important things that are immensely fitting to be something of the past.

In general companies are permitted to observe employee activities by the courts. Private companies have been setting rules in situations when employees are taken into service for instance contracts that affirm that they will be monitoring employees' use of the Internet or any company tools (Chieh and Kleiner, 2003). Efforts have been made in arrangement for laws that protect business and the employees, regrettably most current court cases have been deceiving evidence in the eyes of the magistrates thus confidentiality or privacy laws have been unsuccessful for employees.

It has been recommended that government, big firms and industries and health care systems should have the capability to tape and study workers activities as it is a benefit to research and development for several years. Most legislation is the same opinion that laws should be set in place even though the breach of human rights forbid them from approaching the issue to a law level (Welebir and Kleiner, 2005). Sadly, comprehensible defenses of privacy opposed to security may never be evident from the view point of the law.

Employers' main apprehension is the decrease in productivity, virus attacks/ damaged equipment (i. e. computers), legal charges and loss of classifies data. Employees' major worry is incursion of their privacy, mistreatment of control and precision in their work. A survey conducted in the year 2000, is that sixty two percent of the employees use Internet resources once a day for their private reasons and twenty percent of them use it for at least ten times.

This is why employer is at unease because a large number of workers are using company property for their own use and not for the business purposes. According to Watson (2002) sopports the idea that productivity is what most companies are concerned about such that if employees use them for their own private uses it will negatively affect productivity. It is compulsory for them to put regulations and policies that will help them monitor employees and their activities during working hours.

Some of the main things that companies use are telephone monitoring particularly when personal calls are made, electronic surveillance, drug testing and verification of emails sent externally for private reasons. Reasons why companies make use of policies is for the reason of a decrease in productivity , sensitive material which arise from unpleasant email usage, workplace accidents caused by prohibited drug use, employees bitterness over monitoring of computers and sexual harassment complaints prompted by dating among workmates. 2. 0 Research Objectives R01.

To identify if security and privacy actions affect things like productivity in the workplace/organization R02. To state some of the security and privacy

actions that some companies are implementing in the workplace R03. To analyze whether organizations nowadays are focusing more on prioritizing their security initiatives thus undermining their employees and their personal lives R04. To evaluate if companies are using the right tools, technologies and methods to maintain good quality security and privacy within their organization 3. 0 Research Questions

RQ1. What do organizations hope to achieve by implementing security in their companies? RQ2. What effect does security and privacy actions have on productivity in the organization? RQ3. Do organizations of nowadays focus more on prioritizing their security initiatives hence undermining their employees and their personal lives? RQ4. Do companies use the right methods, technology and tools when they choose security and privacy as a priority? 4. 0 Hypothesis H1. Security and privacy actions increase things like productivity in the workplace. H2.

Telephone and email monitoring, monitored computer web use and surveillance cameras are some of the security actions that some organizations are implementing to their workers. H3. Organizations nowadays are more focused on prioritizing their security initiatives thus undermining their employees' personal lives. H4. For a company to maintain good quality security and privacy within their organization they have to own the right tools, technologies and methods. Theoretical Framework Workplace performance Security and Privacy in the workplace Priorities of the company such as productivity and protection

The independent variable is security and privacy implementation in companies and workplace performance is the dependent variable. Priorities of companies such as productivity and protection are the controlling variables to the results. 5. 0 Achievements gained From Implementing Security and Privacy in the Workplace Organizations hope to achieve a better performance from their employees when they implement security in the workplace. Most companies today in most parts of the world do observe their workers because they have reasonable reasons for doing so.

Since employers are accountable for their employees they have to provide them with a safe and a secure workplace. By monitoring or surveilling employees, employers hope to achieve several things such as employee or customer satisfaction, protection of the company's confidential information and prevent trade secrets from leaking out, non-offensive material from emails and the internet, high performance from the network and the systems and to boost employee productivity (Vorvoreanu and Botan, 2001). 5. Non-offensive material from emails and the Internet According to Lee and Kleiner (2003), employees are responsible for all their workers during employment hours such that even any of the workers happens to send offensive information/materials and they happen to offend the receiver, the employers are the ones who will be liable to this course of action. If the material that would have been sent is found offensive for certain then the company can be sued which can affect the companies' reputation to a greater extent.

To prevent such cases most companies have seen it fit to take the initiative of monitoring each and every email and web use by the employees. 5. 2 Prevention of trade secrets from leaking out According to Paciniet al. (2008),

there are several physical actions that employees consider when doing an internal control to safeguard trade secrets of the company. Such actions include a restriction on accessing certain premises (use of key cards), locks for all file cabinets, surveillance equipment to see all movements and passwords for accessing computers.

Monitoring employees especially when it comes to trade secrets boosts productivity because employees who have intentions to harm the organization are quickly detected and those who are loyal to the company will work to their maximum potential because they know that they are safe.

5. 3 High Performance from Network and the systems of the Company

Companies do not only monitor their employees just to check if they are doing work properly. They also monitor them in order to know if the network and system performance is not being taken advantage of by being used for personal use hence a decrease in productivity.

If a computer network is efficient it is of a great advantage because it increases productivity in the workplace. If a computer system is poor it can be a great loss to the firm because productivity can decrease which results in loss of customers and profits. Most employers really consider the network bandwidth traffic; this is related to employees using the network for personal use . These activities include downloads which decreases network and systems performance, also sharing and use of large audio and video files, surfing the internet and personal emails which are of high volume.

All these actions by employees can cause the network/system be attacked by viruses which may cause it to be disabled (Trim, 2005). Secondly, if the

bandwidth is used for purposes that are not work-related somehow it would be an expense that could have been avoided and to make matters worse the expenses that are incurred do not contribute to the wellness of the firm (Strategic Direction, 2009). For example nowadays most organizations are seeking to adopt the Web 2. 0 technologies for the sake of privacy and security of their companies.

This type of technology according to Almeida (2012), it enables the employers to prevent data loss which would have been caused by inappropriate use of social media applications such as YouTube, Skype during working hours will definitely increase productivity in the workplace. According to Doshi (2009), employer does believe in monitoring their employees because it is a fast and easy method of getting the job done. Productivity and profits increase because the employees will work efficiently and at ease hence a lot of work is done in a short period of time.

When workers work efficiently the employees themselves is satisfied hence customers are satisfied as well (Chan et al. 2005). According to The Gazette (2008), Internet abuse is a rising problem that is costing Canadian businesses beyond sixteen billion dollars yearly in lost productivity and the amount is predicted to be eighty billion dollars in the United States. 6. 0 Security Actions That Most Organizations Are Implementing 6. 1 Drug Testing Most organizations do drug testing for security reasons.

For companies that are doing drug test, they test mainly for alcohol and drugs separately and others test for both. Employees who come to do their job under the influence of drugs/alcohol may be a threat to other work-

mates. Secondly, drug testing has increased because of a rise in health cost and an increase in the danger imposed by lawsuits which come from worker disease. Many companies are involved with drug testing their employees because it is one of the best ways for solving medical and economic problems (Jardine-Tweedie and Wright, 1998) .

According to Lu and Kleiner (2004), if the drug testing by the employer is legal and correctly does things according to the law of that particular state then the company will have to look forward to higher profits. High profits are obtained because the employee will be more productive, higher level of morale, a low rate of absenteeism, low health care and fewer injuries are encountered during working periods. 6. 2 Electronic Surveillance Computers are changing rapidly nowadays especially in the workplaces such that monitoring employees by electric equipment is more common.

Surveillance cameras/ CCTV is another means used by employers to monitor their employees, they are always aware of all the activities that take place in the organization and surrounding areas. According to Chen and Park (2005), monitoring employees regularly would reduce cases of spies in the organization getting away with their actions. Such cases are few because these “ spies” are aware that they are being watched thereby lose interest to do any illegal actions that will jeopardize their identity (Lu and Kleiner, 2004).

Next, management’s main objective is to increase productivity and gain more profit hence they believe monitoring employees’ will improve their productivity levels for the better and an assurance of service of high quality.

Chieh and Kleiner (2003) states that employers can use information they get from the cameras to find out things that are going wrong in the workplace or find out reasons why productivity is decreasing. For example, an employer can discipline workers who may have been wasting their working hours on their own interest based from the information obtained from monitoring.

From this employees are bound to focus more on their assigned duties rather than waste time during working hours. Surveilling employees also motivates them to work even harder than they have been doing (Lee and Kleiner, 2003). Managers can somehow conduct a performance evaluation of their employees whereby they will be able to give a feedback to the employees' and explain which parts needs correction. From monitoring they are able to dictate the type of employees who are hard-working and those who need help.

Employers are also able to detect mistakes the employees are making and from this it will be easy to assist them and correct them. 6. 3 Emails, Voicemails/Telephone calls, Files and Web/Internet use monitoring Many companies monitor employees' emails, files, voicemails and internet use for various reasons. The number of companies who practice this type of monitoring has increased over the past years (Cox et al, 2005). Employers proclaim that by monitoring employees email, voicemails/telephone calls that way they can be certain that they do not contain any materials that can offend the receiver.

Email monitoring is when employers monitor all emails that are going in and out for security purposes to make sure that employees are not disclosing

employment or business confidential information. They may monitor as well to check if employees are not harassing other coworkers. Telephone monitoring is a system of managing calls and observing service by the employees. This type of surveillance is used to monitor employees when they make or receive calls and they can gather information on how the employees are performing.

Internet use monitoring is when managers take the initiative to observe all the steps of their employee's online tracks. Sixty percent of the firms in the United States of America gain from the complex technology and they opt to monitor the workers activities on the Internet (Ciocchetti, 2010). In cases that they are in such situations whereby a worker sends offensive material employees are able to deal with the accused accordingly based on the proof of recorded conversations/videos.

For example, Xerox Company fired forty employees who were caught viewing Pornography sites on the internet during working hours (The Register, 2000). Employers have been monitoring all its employees all over the world (ninety-two thousand in total) by taking records of every web site opened. The main reasons why they were fired is because they spent most of their working hours on issues that were not related to their company and also viewing pornographic sites may have been offending material to coworkers.

Companies have installed different types of technologies just to monitor their employees' activities. Examples include software that filters specific content of information to prevent it from leaving the firm which may lead to the

disposal of company secrets. Other types of software used by companies are those that can monitor log-on and off times so that employers can see if workers are wasting time on issues that are not company related.

Monitoring of emails, voicemails, files and Web use is believed to be another way that makes it certain that employees will work efficiently and possess productive work habits. Productive work habits boosts efficiency which increases productivity thus perfecting customer service. According to Welebir and Kleiner (2005), the worry for organizations is to keep up with the aspect of having power over production and encouraging utilization of the Internet as a priceless resource.

A survey conducted by IntelliQuest Information group revealed that there was an increase in private use of the Internet at work. The results signified that the use of had grown from 6. 9 hours to 9. 8 hours for every week prior to the last year and about fifty seven million workers access Internet from their workplace for private use. Further information provided by the study was that the number of workers seemingly receiving classified information from competitors has increased from 9. 2 percent to 24. percent within a year. Moreover workers are getting emails with attachments, roughly one fifth of the workers have reported receiving insulting email from an inner source and only a third to confess spending more time on the Internet for personal use. States do not have the same policies for monitoring and governing websites viewed by the residents. States like China, Vietnam and Singapore does not only block sites for pornography they also ban access to linguistic and political issues (Hechanova and Alampay, 2010). 7. Prioritizing Security and Privacy Ignores Employees' Personal Lives Opponents of

implementing security and privacy in the organization state that organization nowadays are too concerned with their own company interests and its prosperity thus forgetting that their employees do have personal lives. Installing electronic cameras that will be watching their activities all day when they are at work, monitoring emails and phone calls is making companies seem as if they are forgetting that their employees have a life to live (Dubbeld, 2004).

This side of the coin feels that staff is at liberty to confidentiality when they are using the Internet. Employees argue that as they are allowed to breaks, lunch hours or other selectedperiods where they are not liable to any duties but still in the building they should have the freedom to do things like checking their e-mail, do their banking or shopping and maybe just browse the Internet on free time. Everyone is entitled to some privacy no matter where they are so they argue that they should be able to do this during their free time without anyone monitoring all their movements.

Secondly, employees do not consider it as monitoring productivity when companies even observe staff in the toilet or relaxing areas of the office. Some employees consider it as an intrusion and they have lawful hope that they can maintain their personal lives private. Undermining workers privileges to confidentiality by surveillance and monitoring is not the only problem that employees face. It also generates high levels of stress and nervousness which to higher chances may lead to poor health of workers and a reduction in performance.

Examples of physical wellbeing problems which may be caused by monitoring are repetitive Strain Injury and Carpal Tunnel Syndrome from performance monitoring by the company for instance keyboard strikes. To add on, employees believe thatthey are individuals who can make their own decisions hence it is their right to be treated as proficient andindependentpeople. Guaranteeing their individual development and performance that can be valued is what they believe they can achieve if they are treated as independent people thus they consider surveillance as violating their privacy (Ahmed, 2007).

Workers argue that as long as individual e-mail does not hinder or conflict with business life, it should be permitted. Employees also argue that phone calls take more time than writing an e-mail and also that they should be given time to do individual matters because it can reduce the rate of absenteeism. Most employees have suggested that as long as there is a realistic limit on this practice of monitoring emails, there is no reason for fear but in situations where someone does something unusual then they will have to be dealt with (Kierkegaard, 2005).

Even if employees are informed that they are being monitored and in agreement that they are using company property they still feel that their employers' are not respecting the fact that besides working for tem they also have personal lives which still go on whether they are working or not. 8. 0 Better results can be achieved by using the right tools, technologies and methods For a company to maintain good quality security and privacy within their organization they have to own the right tools, technologies and methods.

A company cannot just instill a rule/wake up one morning with intentions of monitoring all the activities of their employees and expect high productivity. Companies have to follows certain regulations to install such things as software that monitors an employees' Internet use and all phone calls, drug testing and electronic surveillance. A cautiously worded policy that informs employees concerning the necessity of surveillance in the company will be the most probable way that it can gain acceptance or support for workplace monitoring from them (Watson, 2002).

According to Mei-ShaChieh and Kleiner (2003), as regards to other forms of monitoring, it is vital that all forms of surveillance should not be unreasonably intrusive. The methods that employer's use when they consider monitoring employees should be practical because if they are not deemed like that then the company can encounter problems such as rebellious employees; which may cause a decrease in performance. Arnesen and Weis (2007) critically supports the idea that Employers must know that it would not be irrationally intrusive to observe what an employee does in public; however it might be intrusive to observe the employee's behavior hen they are in private places such as the toilet. For example, it may be practical to take pictures of employees when they are at work to observe productivity. However, it may unreasonable to put transparent panels in the ceiling of an employee lavatory. Moreover, if convincing conditions state the use of cameras in locker rooms or other private areas, they are supposed to have signs warning employees they are there. Next, Kierkegaard (2005) states the some of the international regulations and codes that organizations

should take note of when they decide to prioritize security and some form of privacy in their workplace.

The International Labor Office (ILO) has issued a Code of Practice on the Protection of worker's personal data" and it is anticipated to give assistance on the safeguard of workers' private data. The most important requirements of the Code include issues like using individual data legally and justly only for reasons that are directly applicable to the employment of the staff and for the reasons which they were gathered for in the first place. Employers should by all means necessary not keep insightful private information of employees and all employees should be well-informed before such events take place in the organization.

They should be informed of any kind of monitoring that especially the ones that involve personal data collection. However, the information obtained from monitoring them should not be the only issues when doing a performance appraisal. Companies have a duty to safeguard private documents against any kind of a loss, unapproved access, usage, changes or exposure. Employees must have admission to their entire personal information and all rights to scrutinize and get a copy of all the archives.

Revealing an Internet supervising policy is an essential element in an organization. Workers ought to be up to date with the type of activities that would be supervised, the regularity monitoring and how the management will be informed of the activity. If the organization verifies how the employees use their Internet then they must be informed and if the company retains deleted information for reasons like security when they should be

informed about it (Welebir and Kleiner, 2005). The staff should not have beliefs that their actions on the Internet are confidential.

Even though companies do not want to present the idea that they are monitoring each word they key in and mouse clicks on the Internet, it is compulsory to tell employees that they do not own any personal confidential rights when they are using the company Internet. 9. 0 Research Design and Methodology The impact of implementing security and privacy in the workplace and the effect it has on performance in the firm is an ontological study which takes a subjectivism view because security and privacy is created from the perception that workplace performance might be positively or negatively affected.

The research is more of an explanatory studywhich is a deductive approach where Saunders et al. (2006), defines deductive astestinga concept in which the researcher cultivates the concept and assumption and design a research plan to test the assumption. The research strategy that is suitable for this study is survey because according to Saunders et al. (2006), it is usually related to a deductive approach and since we are using companies it is a tactic commonly used in businesses.

I believe the research choice suitable for the study is a multi-method qualitative study whereby semi-structured interviews and questionnaires can be used for data collecting. Time horizon that can be used is a longitudinal study where according to Saunders (2006), the researcher embarks on a study at numerous facts in time in order to answer a research question. For reliability and validity sake to how security and privacy affect workplace

performance several times of embarking on such a question will provide accurate results. Physical access is the one suitable for my study since I am an external researcher.

Access would be granted from the management of all the companies that are to be used for the study and gaining an informal access from all the employees for accurate results. One of strategies that can be used to gain this access is that the project will benefit the company in one way or the other. Research ethics that should be maintained during data collection stage are confidentiality and anonymity. Furthermore, the sampling method technique I used is probability specifically cluster sampling is what I would consider because there are specific types of jobs that make use of surveillance cameras, computers (with internet) and telephones. . 1 Possible Results Based on the literature analysis, H1 can be accepted because by implementing security in the workplace it can work in two ways. Firstly, protects the business from competitors and can be used when evaluating employees. H2 can also be accepted because not only American companies use Surveillance cameras, do telephone and Internet monitoring, companies in Europe and in countries like China, Vietnam, Philippine, Australia also do the same. H4 is acceptable because for the policy of applying security and privacy to work companies have to follow proper procedures.

However H3 will remain debatable in the sense that in every topic that arises there is always going to be a group of people who will rebut the idea. It is acceptable only when the company does not communicate the use and the reasons behind the monitoring. 10. Conclusion Based on the evidence and facts from the literature review which provided various perspectives about

security and privacy it can be concluded that monitoring employees can result in something noble or something unscrupulous.

For example, emails and surfing the Internet can be a disruption but at the same time the feeling of being watched regularly can also be a disruption. Law of privacy has to balance employee interest against those of the employers and more prominently it must center on the important concepts of human self-esteem. Information technology has assisted firms to enlarge their productivity and efficiency but the misuse of the Internet has steered firms to monitor all communications operated electronically to guard their companies and limit legal responsibilities.

Nowadays two major developments to be concerned about in regards to electronic surveillance is the great concern for employee privacy and the increased cases of employers being caught accountable for workers' misbehaviors of electronic communication. Although the courts are in support of employers they must be alert about the workers' rights though shielding the firms' interests. Words 4 282 References Ahmed, S. (2007). Analysis of Workplace Surveillance In a Quest for an Ethical Stance. Journal of Business Systems, Governance and Ethics, Vol 2, No. 4. Almeida, F. 2012). Web 2. 0 Technologies and Social Networking Security Fears in Enterprises'', International Journal of Advanced Computer Science and Applications, Vol. 3, No. 2, Amicus Guide. (2005). Amicus Guide to Privacy at Work. Privacy at Work. [Online]. Retrieved on 19 March 2012 from: http://www. amicustheunion. org/pdf/PrivacyatWork. pdf Arnesen, D. W and Weis, W. L. (2007). Developing an Effective Company Policy For Employee Internet And E-Mail Use. Journal of Organizational Culture, Communications and Conflict,

Volume 11, No. 2, pp. 53-65. Chen, J. V and Park, Y. 2005) “ The role of control and other factors in the electronic surveillance workplace”, Journal of Information, Communication and Ethics in Society, Vol. 3 Iss: 2, pp. 79 – 90. Ciocchetti, C. A. (2010). The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring. [Online]. Retrieved on 19 March 2012 from: http://www. futureofprivacy. org/wpcontent/uploads/2010/07/The_Eavesdropping_Employer_ %20A_Twenty-First_Century_Framework. pdf Cox, S; Goette, T. and Young, D. (2005). Workplace Surveillance and Employee Privacy: Implementing an Effective Computer Use Policy, Volume 5 Issue 2. Dubbeld, L. 2004) “ Limits on surveillance: Frictions, fragilities and failures in the operation of camera surveillance”, Journal of Information, Communication and Ethics in Society, Vol. 2 Iss: 1, pp. 9 – 19. Guha, M. (2008). “ The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets without Compromising Employee Privacy or Trust”, Library Review, Vol. 57 Iss: 9, pp. 746 – 747 Hechanova, R. M. and Alampay, E. A. (2010). Monitoring Employee Use of the Internet in Philippine Organizations’’, The Electronic Journal on Information Systems in Developing Countries, Volume 40 Issue: 5, pp. -20. Kierkegaard, S. (2005). Privacy in Electronic Communication. Watch your e-mail: your boss is snooping. Computer Law & Security Report,” Vol. 21 Iss: 3, pp. 226-236. Lee, S. and Kleiner, B. H. (2003). “ Electronic surveillance in the workplace”, Management Research News, Vol. 26 Iss: 2/3/4, pp. 72 – 81. Mei-ShaChieh, C. and Kleiner, B. H. (2003),” How organisations manage the issue of employee privacytoday”, Management Research News, Vol. 26 Iss: 2 pp. 82 – 88. Petrovic-Lazarevic, S. and Sohal, A. S. (2004). “ Nature of e-business ethical dilemmas”, Information Management & Computer Security, Vol. 2 Iss:

2, pp. 167 – 177. Rustad, M. L. and Paulsson, S. R. (2005). Monitoring Employee e-mail and Internet Usage: Avoiding the Omniscient. Electronic Sweatshop: Insights from Europe. U. Pa. Journal of LaborAnd Employment Law, Vol. 7: 4. Saunders, M. , Lewis, P, and Thornhill A. (2006) Research Methods for Business students. 4th edition . UK: Prentice Hall. Strategic Direction. (2009) " Social networking and the workplace: Making the most of web 2. 0 technologies", Vol. 25 Iss: 8, pp. 20 – 23. The Gazette (2008). ' Stealing' time at work on Net.

One of the new trends to watch in labor law is how companies and labor tribunals handle cyberslacking- a term coined to describe people who spend an excess of time on the Internet at work. [Online]. Retrieved on 31 March 2012 from: http://www. canada. com/montrealgazette/news/business/story. html? id= 32125d78-a479-497a-ae19-4f461ea18060 The Register. (2000). Xerox fires 40 in porn site clampdown. Document Company staffs get caught shuffling more than just paper. Trim, P. R. J. (2005). " Managing computer security issues: preventing and limiting future threats and disasters", Disaster Prevention and Management, Vol. 4 Iss: 4, pp. 493 – 505 Vorvoreanu, M. and Botan, C. H. (2001). Examining Electronic Surveillance In the Workplace: A Review of Theoretical Perspectives and Research Findings. [Online]. Retrieved on 16 March 2012 from: http://www. cerias. purdue. edu/assets/pdf/bibtex_archive/2001-32. pdf Warren, A. (2002) " Right to privacy? The protection of personal data in UK public organisations", New Library World, Vol. 103 Iss: 11/12, pp. 446 – 456. Warren, M. J. (2002). " Security practice: survey evidence from three countries", Logistics Information Management, Vol. 15 Iss: 5/6, pp. 347 – 35. Watson, G. (2002).

E-mail surveillance in the UK workplace-a management consulting case study", Aslib Proceedings, Vol. 54 Iss: 1 pp. 23 – 40. Welebir, B. and Kleiner, B. H. (2005)," How to write a proper Internet usage policy", Journal of Management ResearchNews, Vol. 28 Iss: 2 pp. 80 – 87. Whalen, T. and Gates, C. (2010)," Watching the watchers: " voluntary monitoring" of infosec employees", Journal of Information Management & Computer Security, Vol. 18 Iss: 1 pp. 14 – 25. Moghe, V. (2003) " Privacy management – a new era in the Australian business environment", Journal of Information Management & Computer Security, Vol. 1 Iss: 2, pp. 60 – 66 Ying-Tzu Lu, Brian H. Kleiner, (2004)," Drug testing in the workplace", Journal of Management Research News, Vol. 27 Iss: 4 pp. 46 – 53 Jardine-Tweedie, L. and Phillip C. Wright, (1998) " Workplace drug testing: avoiding the testing addiction", Journal of Managerial Psychology, Vol. 13 Iss: 8, pp. 534 – 543 Chan, M; Woon, I. and Kanakanhalli, A. (2005). " Perceptions of Information Security in the workplace : Linking Information Security climate to Compliant Behavior", Journal of Information Privacy and Security, Volume 1 Issue: 3, pp. 8-41 Chieh, C. M. and Kleiner, B. H. (2003), " How organisations manage the issue of employee privacy today", Journal of Management Research News, Vol. 26 Iss: 2 pp. 82 – 88 Bibliography Gritzalis, S. (2004). " Enhancing Web privacy and anonymity in the digital era", Journal of Information Management & Computer Security, Vol. 12 Iss: 3, pp. 255 – 287. Griffiths, M. (2010)," Internet abuse and internet addiction in the workplace", Journal of Workplace Learning, Vol. 22 Iss: 7 pp. 463 – 472 Morgan, C. (1999).

Employer Monitoring Of the Employee Electronic Mail And Internet Use. McGill Law Journal, Vol. 44 pp. 850-902. Jardine-Tweedie, L. and Phillip C.

Wright, (1998) “ Workplace drug testing: avoiding the testing addiction”, Journal of Managerial Psychology, Vol. 13 Iss: 8, pp. 534 – 543 Appendices

Appendix 1: Evaluation of Sources In order to do my literature review I made use of secondary data which consisted of journals, books and web publications (which included newspapers). From these sources I could get dependable information because they are reliable sources.

I did not manage to get a lot of recent journals for the current year and for the previous year but I did manage to get publications which were within the ten years. These sources really helped me understand more facts about my research topic. Most of the journals that I found were useful to explain my topic and write more facts because they had information that I wanted to use. Most of the journals that I found discussed reasons why organizations were implementing security and privacy in their organizations and the proper procedures that were supposed to be taken for such policies.

However it was not easy to get journals that rebuttal those ideas and supported that somehow it affected employees. Secondly, I was able to find journals that explained security and privacy from companies in different countries. The issue of security and privacy in the workplace was more crucial beginning 1996 which shows that it’s an issue that that was brought about technology advancements. I found most of my journals on emerald insight and to top it up I found more from scholar web publications. I took my time to paraphrase all the necessary information from the journals that I found to support all my assumptions.

I used twenty- three journals to support my ideas, except for one journal all of them the author name was given, dates, journal article headings and all the information needed to do the referencing. The impact of implementing security and privacy and its effect on workplace performance Appendix 2: Mind Map Week 1 Received topics to research on Week 2 Search for relevant journals mainly from Emerald Insight. com Week 2 Research Objectives Research Questions Hypothesis Week 2 Chose the research topic Week 3 Theoretical Framework Introduction & Search for more Journals

Week 4 Non-offensive material from emails and the Internet High performance from company networks &systems Week 4 Protection of company confidential information Prevention of trade secrets from leaking out Week 4 Positive effects of security and privacy mainly on productivity, employee &customer satisfaction Week 5 Security & Privacy actions that companies are using Week 6 Facts raised by opponents of Security and privacy e. g. electronic surveillance Week 7 Owning the right tools, technologies and methods Week 9 Research Design and Methodology Possible Results