SOFTACTIVITY.com
You see what they do

Employee Monitoring

An essential component of your risk management strategy

Rhonda Turner
Sponsored by Deep Software Inc.

While the internet has presented organizations with an extraordinary array of new opportunities, it has also presented them with an equally extraordinary array of new challenges – and risks. Whether an organization is a multinational corporation or a small family-owned company, misuse and abuse of the internet, e-mail and instant messengers can impact on staff productivity and result in potentially costly legal headaches.

This white paper will explain why organizations need to monitor their staff's computer activity and provide some practical guidance on how they can do it right.

Deep Software Inc.
#250-625 Agnes Str.
New Westminster, BC, Canada
V3M 5Y4

www.softactivity.com

CONTENTS

INTRODUCTION

With so much of today's commerce being conducted electronically, providing staff with internet access has become a business necessity. The internet, e-mail and instant messaging have become essential tools that staff use to communicate, collaborate and carry out research.

Yesteryear, it was relatively easy for organizations to create Acceptable Use Policies (AUP's) that clearly specified permissible uses for internet and e-mail. The evolution of Web 2.0 has, however, made that a much more difficult process. Wikis, weblogs, forums, social-networking websites and instant messaging are no longer strictly leisure time technologies – they have become vital business resources used in marketing, research and communication and collaboration. But they are resources which can also be misused or abused. How much time do your employees spend surfing the internet ("cyberslacking")? What do they do during their time online? Search for the best vacation deal, visit an internet casino or look for their perfect partner? How many of the e-mails that are sent and received are work related and how many are forwarded jokes and videos that unnecessarily consume both the employee's time and the company's bandwidth? Do employees use e-mail to harass their colleagues? Do employees obtain information from the organization's network and use that information for immoral or illegal purposes?

Lost productivity is not the only computer-related risk that organizations face. The improper use of e-mail and instant messengers can lead to extremely expensive lawsuits, and the proliferation of mobile devices has made it considerably easier for errant employees to steal sensitive information.

This white paper will detail the risks to which organizations that do not monitor their employees are exposed and explain the right way for organizations to go about monitoring.

WHY YOU NEED TO MONITOR YOUR EMPLOYEES COMPUTER ACTIVITIES

The monitoring of employees is commonplace. The majority of employers monitor employee arrival times. The majority monitor that cash has been handled correctly. The majority monitor the accuracy and quality of employees work. Monitoring in this manner is accepted as a business necessity and most organizations would consider it completely irrational not to make such checks. Yet, a surprisingly large number of organizations still do not adequately monitor the manner in which employees use their computers – and that can be an extremely costly omission. The misuse and abuse of computer equipment can have serious consequences for an organization:-

- **Lost productivity**

  Personal surfing has become an enormous problem for employers. Employees shop, gamble, play games, chat, watch and share videos and visit online red-light districts – all during working hours. Estimates as to the amount of time that is lost to cyberslacking vary enormously, but most studies put it in the region of 2.5 hours per employee, per day. Multiply that 2.5 hours by the number of employees and the average hourly pay rate in your organization, and you will have a ballpark estimate of the cost of cyberslacking. It's probably more than you thought, huh?

  Social networking site, Facebook, was recently dubbed a *social not-working* site after a study by security company Sophos revealed that 60% of its users accessed the site during working hours – and that more than 20% of its users accessed the site more than 10 times each day during working hours.[1] There are more than 51 million Facebook users and that number is increasing by more than 200,000 per day. How many Facebooking cyberslackers are in your organization and how much are they costing?

A recent study by Carnegie Mellon University's Software Engineering Institute found that 75% of IPT's were carried out by current members of staff.

- **Intellectual property theft**

  Intellectual property theft (IPT) has always been a concern for companies – and internet-connected computers and mobile devices provide new opportunities for people to access and steal data. Documents and data can easily and speedily be transferred to a flash drive or laptop. Many organizations are concerned about outsider theft, but, in fact, the majority of thefts are committed

by insiders. A recent study by Carnegie Mellon University's Software Engineering Institute found that 75% of IPT's were carried out by current members of staff.

Companies often do not admit to being victims of IPT, and so it is impossible to quantify the costs. The sums involved can, however, be considerable. In a recent case, a research chemist admitted to stealing $400 million worth of proprietary data from his former employer, DuPont.[2]

- **Fraudulent activity**

  Employees often have access to sensitive personal information which can either be misused by the employee or sold on to a third party. HSBC customers had almost $500,000 stolen from their accounts after an HSBC employee passed on data to criminal associates[3]. A Social Security employee in the US sold personal information that was used in a $2.5 million identify theft scheme.[4]

  The cost of fraudulent activity extends beyond the losses incurred as a direct result the fraud – the financial effects of the damage to an organization's reputation and the loss of customer confidence can far outweigh the cost of the fraud itself.

- **Legal liability**

  In most jurisdictions, employers hold some form liability and accountability for the actions of their employees. According to the ePolicy Institute, 13% of employers have been faced with a lawsuit resulting from the improper use of e-mail by employees[5] - and such lawsuits can be extraordinarily expensive. Petrochemical company Chevron were ordered to pay $2.2 million to settle a sexual harassment claim that stemmed from inappropriate e-mails circulated by male employees.[6]

From multi-million dollar lawsuits and settlements to public embarrassment and public relations disasters to deliberate sabotage and industrial espionage, the list of risks to which organizations are exposed is practically endless. Monitoring your employees computer activities is not a big brother tactic, it's responsible business and helps protect both an organization and its stakeholders – including its employees.

MONITORING: HOW TO DO IT RIGHT

Monitoring employees should not in itself be regarded as a panacea to the problems previously discussed. To be effective, monitoring must be introduced as part of a risk management strategy that includes:-

- **ePolicy**

  Organizations should create an AUP that covers e-mail, internet and applications and that AUP should be clearly communicated to employees. Should an organization fail to create or communicate an AUP, it will be exposing itself to a myriad of legal problems. In a case in the UK, IBM lost an unfair dismissal case brought by a former employee who had been sacked for using company computers to access pornography. The Tribunal decided that there had been no clear breach of company policy and the former employee was awarded compensation. In order to avoid such complications and potentially costly legal battles, an AUP should:-

  - Be communicated to staff in writing
  - Clearly set out permitted and prohibited uses for e-mail, internet and applications
  - Specify the disciplinary consequences of breaching the AUP
  - Explain the employer's right to monitor and explain what will be monitored

  Explaining that a monitoring mechanism is in place is important for a number of reasons. Firstly, failing to advise employees that their computer activities will be monitored may be an infringement of their privacy rights in certain jurisdictions. Secondly, if employees are aware that they are being monitored, they are less likely to breach the AUP – and prevention is better than cure. Thirdly, undisclosed monitoring would invariably negatively impact on staff morale. There may be occasions when unannounced monitoring is deemed necessary, but such action should not be taken without careful consideration and, if there is any doubt as to the legal implications, advice from a qualified professional.

The AUP must be carefully drafted and make absolutely clear what is and is not permissible. Do you want to impose a blanket ban on personal surfing? Or permit it only during coffee and lunch breaks? Do you want to prohibit the use of peer-to-peer applications? What type of content should employees be prohibited from accessing? To what extent should employees be permitted to send personal e-mail? Unless the AUP is specific about permissible activities, an organization could find itself facing a costly and time consuming claim for unfair dismissal.

- **Education**

  The AUP should be supported with a company wide education program that sets out:-

  - The reasons for the AUP
  - That compliance is mandatory
  - The conditions of the AUP
  - The consequences of non-compliance
  - The extent of monitoring
  - Who an employee should approach with any questions about the AUP

  An education program will not only clarify the AUP to employees and help ensure compliance – it may also provide a defence against lawsuits by enabling an organization to demonstrate to the courts that all reasonable steps were taken to ensure that the workplace was free from harassment and non-hostile.

- **Technology**

  You wouldn't trust your employees not to steal from the cash register simply because you had informed them not to – and nor should you trust your employees to voluntarily comply with the AUP. Most will, but some will not. Most organizations have found it necessary to either discipline or dismiss staff because of their misuse or abuse of computer equipment – and, if your organization has not yet found such action necessary, chances are that's because you do not have the technology in place to enable you to discover breaches of the AUP.

  To be effective, an AUP must be underpinned with a monitoring mechanism. Should it not be, some employees will intentionally or unintentionally fail to adhere to the rules – and that is something which could prove to be extremely costly.

ABOUT ACTIVITY MONITOR

Deep Software's Activity Monitor is a program that provides comprehensive monitoring and reporting functions. Activity Monitor consists of a server-side application and a client-side application that can be remotely installed on any computer in the network and is completely invisible to the end-user. For any computer on which the client application is installed, you can:-

- View the desktop in real time
- Monitor and log websites visited
- Track application usage
- Record e-mail sent and received
- Record chats in IM programs
- Record keystrokes in real time
- Remotely control the computer
- Schedule screen captures
- Store activity logs in a centralized location
- Export logs to HTML or Excel
- And much more

Activity Monitor will provide you with all the information you need to be able to enforce your AUP and will help you:-

- Eliminate cyberslacking and boost productivity

"We love this program it is the best program we have used and we have tested quite a few. It has helped tremendously in our silent monitoring of the customer services reps. Now the manager/team leaders can see what is happening while the customer is speaking with the rep. and can provide guidance on how to improve our systems or service."

-JR Williams, Uline, System-Network Engineering Lead

- Minimize the risk of ITP
- Avoid expensive workplace lawsuits
- Prove grounds for disciplinary action and avoid claims of unfair dismissal
- Protect your employees from harassment and bullying

In short, Activity Monitor will help you protect sensitive and proprietary information, protect your employees, protect your organization's reputation and, ultimately, help protect the bottom line.

ABOUT DEEP SOFTWARE INC

Based in New Westminster, BC, Canada, Deep Software Inc. specialises in the development of security products and web analytics software for large enterprises, small and medium-sized businesses, as well as home PC users. Activity Monitor is developed by SoftActivity, a division of Deep Software Inc. The company has 8 years experience in this field and were one of the first companies to develop this type of product.

To find out more about Deep Software and its products, please visit www.softactivity.com or www.deep-software.com.

ABOUT THE AUTHOR

Rhonda Turner is a Vancouver Island-based technical consultant and writer. Rhonda has worked with numerous leading international technology companies and has authored papers and articles on subjects ranging from virtualization to PCI DSS compliance. To contact the author e-mail: rhonda@mvps.org.

RESOURCES

[1]One in seven brings their Facebook addiction to work (Sophos)
http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-addiction.html

[2]Massive Insider Breach At DuPont
http://www.informationweek.com/news/showArticle.jhtml?articleID=197006474

[3]HSBC Bangalore suffers £233,000 security breach
http://news.zdnet.co.uk/itmanagement/0,1000000308,39277837,00.htm

[4]Social Security Administration Worker Charged In Identity Theft Scheme
http://www.informationweek.com/news/showArticle.jhtml?articleID=199000813

[5]ePolicy Institute
www.epolicyinstitute.com

[6]Chevron Settles Sexual Harassment Charges
http://query.nytimes.com/gst/fullpage.html?res=990CEFDB1738F931A15751C0A963958260