South African Journal
of Information Management
[DoE accredited]

Peer Reviewed Article

Vol.6(3) September 2004

Managing employee Internet abuse

Anesh Maniraj Singh
Information Systems and Technology, University of Kwazulu Natal-Westville
anesh@consultant.com

Contents

Key words: Internet abuse, common types of Internet abuse, remedies for Internet abuse, Internet usage policies, managing Internet abuse

1 Introduction

The Internet and the World-Wide Web have heralded a new era in communications and the way modern business is conducted. Communication can take place 24/7/365, around the globe to millions of people, within seconds for a fraction of the cost of using postal or telephonic communication. Similarly, business can be conducted anywhere in the world from the comfort of one's home or office without incurring the cost of having to travel to business clients or associates. These among many other things are some of the benefits that accompany the Internet. However, with the benefits, there are a number of challenges that arise as well. Hacking, fraud, pornography, viruses, spying, and spam are among the more popular cyber crimes. Reading the recent daily press, one is more often encountering headlines such as: 'Employees dismissed for sending hate mail', 'Employees spending excessive time on pornographic sites' and 'Companies invading staff e-mail privacy'. This type of publicity is exposing the fact that Internet facilities and Internet usage need to be regulated in order to strike a balance between the rights of individuals and the rights of organizations. This article reports on research that examined employee Internet abuse and how it can be managed while respecting the rights of the employer and the employee. The following issues were examined: common abuses of Internet facilities, impact of abuse on employers, remedies for Internet abuse, the need for Internet usage policies, the legal implications of policies and the contents of an Internet usage policy.

top

2 Rights of the parties

As mentioned, a challenge facing organizations with regard to Internet use is the protection of the rights of the employer and the rights of the employee. With the highly competitive business environment facing organizations, the protection of critical data is a top priority. Employers therefore have to take measures to protect information from getting into the wrong hands. Competitors that have strategic information about an organization could easily use that information to destroy it. Similarly, client information is confidential – if that information is not protected, it could result in expensive litigation. Cost containment and increased productivity are also vital to the success of an organization. Therefore, organizations have to control employee use of corporate Internet facilities.

However, as much as an organization has to protect its rights, it cannot withdraw the rights of its employees. Employees have a right to associate with whomever they want. If this right to association requires electronic communication, it cannot be denied without good reason. Furthermore, an employee is entitled to his or her privacy. Therefore, as much as a company may argue that it has to monitor all electronic communication to protect its rights, it has to also observe the privacy rights of its employees.

In trying to balance the rights of the parties, it is important to distinguish between what is considered use and what is considered abuse.

top

3 Common abuses of Internet facilities

Employees spend many hours on the Internet surfing for information, and sending e-mails. In many cases, employees are using the facilities innocently without the intention of abusing the privilege. However, it has been estimated that in South Africa some 10 to 20% of employees abuse corporate Internet facilities (Israelstam 2001). Seventy per cent of abuse involves the visiting of pornographic sites, and cyber loafing accounts for some 30 to 40% of lost productivity (Conlin 2000). According to Israelstam (2001), closer to home, Internet abuse includes:

- *Using the Internet to send hate or flame mail:* employees use employers' e-mail facilities to send defamatory messages about colleagues and managers, resulting in defamation suits and generally low staff morale.
- *Employees enter into electronic contracts 'on behalf' of the company:* although not a major abuse, employees sometimes enter into contracts without the requisite permission, resulting in the delivery of products and services that do not get paid for. Disputes arise between the employer, the employee and the third party who expects payment.
- *Conducting personal business during working hours:* a commonplace abuse of corporate Internet facilities. Employees use e-mail facilities to send quotations for personal products and services they wish to sell. Others use the Internet to search for prices of music, books and cars among other things. And some use the Internet to conduct their studies.
- *Downloading extremely large files:* a common abuse by younger members of staff who download music, games and graphic files.

Internet usage has to be managed because Internet abuse can impact negatively on organizations.

top

4 Impact of Internet abuse on organizations

Internet abuse is a cost to the employer due to direct costs of the link to the Internet. In large organizations, Internet costs are seldom linked to the benefits. Therefore, it is very difficult to quantify what is acceptable use and what is abuse. In small businesses it is not acceptable to allow employees open access to the Internet.

Employees who sit on the Internet for long periods are not engaged in their normal duties and productivity suffers.

Employers face costly litigation in defamation suits due to e-mails originating from their premises. In 2002 a disgruntled employee of the University of Durban Westville sent out a defamatory e-mail to all members of staff where he accused certain union members of conspiring with the university council, and making admissions of owning private businesses among other issues. Staff who were implicated in the e-mail brought up charges against the individual and the institution. If the incident had reached the courts the institution may have had to accept vicarious liability for the actions of the employee.

The sending and receiving of large files absorb bandwidth which severely hampers the performance of the Internet connection, slowing it down to the point that it could affect users who are legitimately using the Internet for work purposes. This could lead to lower productivity, frustration and poor staff morale.

What should employers do to manage employee Internet abuse?

top

5 Remedies for Internet abuse

There are many remedies to curb Internet abuse, some are discriminatory such as allowing only certain employees to use the Internet, or limiting access to the Internet, others are unconstitutional such as monitoring and others are balanced such as disclaimers and policies. However, overly restrictive policies can lead to employees deliberately wanting to break the policies, or look for loopholes in them.

5.1 Limited authorized access

If an organization has facilities such as the Internet that can empower, educate and improve an employee’s working conditions, it would be discriminatory to allow only certain privileged employees the use of that facility. According to Alge (2001), employers should allow employees personal Internet time; exercising excessive control impedes ideas and innovation. The Internet is a productivity tool in that it makes communication quicker and more efficient. As a learning tool, the Internet gives employees access to new knowledge, which makes them better in their jobs. Employees become both more effective and efficient. This increases their self-esteem, which improves customer service and interpersonal relationships. Therefore, it is not only discriminatory to allow only some employees access to the Internet, but it is also being selfish. However, in SMMEs, cost containment is of the essence, providing free Internet facilities to all employees, all day, will most certainly have a negative impact.

5.2 Monitoring

To protect the business interests especially against industrial espionage, harassment, discrimination, reduced productivity and defamation, employers are resorting to monitoring of employees e-mails and sites visited. According to Conlin (2000), companies are using Web monitoring software that records an employee's e-mail sent and received and the sites visited. She states further that some of the software is capable of ringing 'alarm like' bells to alert management when employees are visiting pornographic sites. In South Africa, the *Constitution* and the *Interception and Monitoring Prohibition Act*, Act 127 of 1992, protect the rights of employees in terms of freedom of speech and the right to privacy. What recourse then does the employer have to protect his or her rights?

The recent *Access to Information Act* of 2002 promotes transparency and allows persons to legally demand the right to examine documents, including electronic documents, where that party can show that the information contained therein may prejudice themselves. Therefore, employers resorting to monitoring have to show just cause for why monitoring is necessary in their organization.

According to Makhanya (2001), due to the increase in Internet crime, the SA Law Commission has asked for an amendment to the *Interception and Monitoring Prohibition Act* 127 of 1992, where the SAPS, SANDF, the Intelligence Agency and the Secret Service have the right to intercept and monitor any communication. This could give employers more protection in terms of protecting information of a strategic nature from being leaked out.

5.3 Disclaimers

To reduce vicarious liability for the actions of employees, employers are appending disclaimers to all e-mail sent from corporate servers. The disclaimer is intended to distance the employer from the contents of the e-mail to prevent the company from being implicated when hate mail, discriminatory statements, harassing statements and electronic contracts are entered into. The disclaimer, although not strong enough to withstand legal scrutiny, serves as a deterrent and silently encourages employees to act responsibly.

Of the remedies recommended above, Israelstam (2001) is of the opinion that a sound Internet policy would be of greater benefit than adopting measures that could in themselves be controversial, and of greater detriment to an organization than the actual offence itself. The author concurs with this approach.

top

6 What are policies and why are they important?

Policies are the implementation of day-to-day rules that put boundaries around what can and what can't be done (Stoner and Freeman 1992). It is evident from this definition, that policies are needed to regulate activities, especially regular activities. They take the form of rules that stipulate what can be done and what can't be done by employees. For example, Aids policies are rules regarding how staff suffering with Aids should be treated and covers issues such as non-discrimination against Aids sufferers, the support and counselling for sufferers, and time off for treatment. An Internet policy is no different from any other organizational policy. Internet policies or Internet usage policies are designed to regulate the day-to-day usage of Internet facilities. Internet policies are designed to protect the rights of the employer and the employees, with regard to the use of Internet facilities. In many instances, policies are developed to ensure fairness and equity in the employer–employee relationship. As much as Internet abuse may seem to be an IT issue to be managed by the IT department, it is a labor relations issue which needs to be handled by line management. However, very few cases of Internet abuse are taken to the CCMA or the Labor Courts, which has resulted in no clear pattern in case law, or precedents being set (Israelstam 2001). Successful policies need senior management support and must be driven from the top even though the development of the policy is a consultative process.

top

7 Legal implications of policies

Before developing an Internet usage policy, it is important for organizations to consider the legal implications and the underlying legislation that will impact on their policies. The following are the current legislation that has to be adhered to when developing an Internet usage policy:

- *Labor Relations Act:* The LRA has specific clauses that allow employees freedom of association. These rights and freedoms have to be incorporated into an Internet usage policy.

- *Electronic Communications and Transactions Act:* ECTA sets out what is considered sensitive information and how employers can protect themselves from cyber crime. It also provides guidelines on individual privacy and how privacy should be managed.

- *Interception and Monitoring Prohibition Act* : This Act is interesting in that it only allows the police, defense force and internal security to monitor communications. However, this act could be amended to allow other parties to intercept and monitor communication.

- *Constitution* : The *Constitution* allows people the freedom of speech and the right to privacy. This places a constraint on employers trying to develop policies limiting such actions.

- *Access to Information Act* : This Act specifies what information can be made available to persons requesting it and what should be kept confidential.

To develop a balanced Internet usage policy, it is evident that existing legislation has to be consulted and the principles incorporated not to breach the rights of the parties.

top

8 Contents of an Internet usage policy

An Internet usage policy or acceptable use policy (AUP) is a verbal or written agreement where all parties promise to use the Internet for the common good (Mitchell 2001). Therefore, an AUP should clearly state who are the parties affected by the policy, what is acceptable usage, what is unacceptable usage, and what are the consequences of unacceptable usage. There should also be provision made for resolving disputes arising from the implementation of the policy. It may seem strange that a policy should state who the affected parties are. However, the modern organization uses consultants, outsource vendors, temporary staff, seconded staff and in tertiary institutions – adjunct staff. Therefore, the policy has to be clear on who is covered and subject to the policy. According to Mitchell (2001), an Internet acceptable usage policy (IAUP) should among other things address issues such as:

- *Passwords* : there has to be clear guidelines with how often passwords should be changed, and the format that passwords should take such as a combination of characters and numerals. This is necessary to prevent outsiders or imposters from accessing an employee’s computer and then stealing, destroying or editing information.
- *Interpersonal etiquette* : this deals with issues such as what is considered appropriate or inappropriate language contained in an e-mail. This aspect should also advise employees not to send offensive attachments or jokes that may cause 'psychological injury' to the receiver.
- *Overuse and misuse of resources* : limits should be placed on file sizes and types of files that can be downloaded or transmitted. Employees must be aware that they should not be using corporate Internet facilities for personal use during working hours, if at all. Furthermore, they should be warned against using company facilities for conducting any criminal activity against the company or any other person or persons outside the company.
- *Time frames for the storage of unread e-mail* : information overload can hamper the effective operation of corporate servers; therefore, if employees do not manage their information, the company should have the right to dispose of it.

According to Alge (2001), an IAUP should be developed in consultation with employees and/or their representative bodies in order to encourage buy-in and acceptance. Furthermore, according to Whiteley (2002), an Internet usage policy should not be an obscure document hidden in a staff manual. The IAUP should be aggressively promoted on electronic bulletin boards, Intranets, notice boards, in training sessions and as part of the induction programme of new employees. Ideally, the policy should be read and signed by the employee that he/she has understood and accepts the contents thereof.

top

9 Who is responsible for managing Internet abuse?

There are many debates regarding who is responsible for the management of Internet abuse. There are those who believe it is an Information Technology (IT) function, others claim it is a human resources issue, while some believe it to be a line management function and some even believe it should be an external audit function. It is most certainly not an IT function. The IT department must provide the infrastructure and reports showing the abuse, they do not and should not have the responsibility of managing the problem. Human resources departments should only advise and guide in the development and implementation of policies. External auditors cannot be expected to perform such a function as it will be a costly exercise. Ultimately managing resources is a line management function. When expenses rise and productivity drops, line management is held accountable. Therefore, line managers have to take the responsibility for managing Internet resources. In order to quantify and make the offences more meaningful, line managers need to receive information on Internet costs incurred per employee. This, coupled with usage logs highlighting non-essential or unofficial usage, will provide a clear guideline for line managers to take the necessary action.

top

10 Conclusion

It is evident that uncontrolled usage of the Internet can expose the employer and employee to costly litigation. The remedies that have been recommended have their benefits and problems. However, to protect the rights of the employer and employee, a policy that controls Internet usage is a very useful tool. Policies have their problems as well, in that they can be overly restrictive, or remain unused on shelves. However, it is a starting point that acts as a deterrent that could reduce Internet abuse and protect the employer, as opposed to having no protection at all. To be fair to both parties, it is recommended to attempt to balance control with discretion. A policy is only as good as its implementation. Once adopted, a policy must undergo regular revision to keep abreast of the changing landscape.

top

11 References

Alge, B. J. 2001. Can corporate security, privacy coexist? [Online]. Available at www.newswise.com/articles/2001/5/privacy2.pur.html

Conlin, M. 2000. Workers, surf at your own risk. [Online]. Available at www.business.com:/2000/00_24/b36825257.htm?scriptframed

Israelstam, I. 2001. Internet exposes employers to abuse. *The Star*, 08 May 2001. Independent Newspapers. [Online]. Available at http://www.iol.co.za/index.php?set_id=3andclick_id=131 andart_id=ct20010508145511599914055O

Israelstam, I. 2001. Not having a net policy can be costly. *The Star*, 15 May 2001. Independent Newspapers. [Online]. Available at http://www.iol.co.za/index.php?set_id=3andclick_id=131 andart_id=ct20010515145509310114O826

Makhanya, P. 2001. Outcry for Big Brother law for Internet. *The Mercury*, 26 July 2001. Independent Newspapers.

Mitchell, B. 2001. The acceptable use policy (AUP). [Online]. Available at http://intranets.about.com/library/weekly/aa021700a.htm

Whiteley, C. 2002. Internet and e-mail policies. [Online]. Available at www.hobsonaudley.co.uk./text.cfm?idvar=176

Disclaimer

Articles published in SAJIM are the opinions of the authors and do not necessarily reflect the opinion of the Editor, Board, Publisher, Webmaster or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special, incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user's use of the Website.

top

ISSN 1560-683X

Published by InterWord Communications for the Centre for Research in Web-based Applications,
Rand Afrikaans University