Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Managing Internet Use: Big Brother or Due Diligence?

Internet access has become an established business tool, taken for granted along with email, telephone and facsimile. Like these other media, giving staff access to the Internet has risks - will they spend all day downloading porn or swapping chat messages with their friends? Will they infect the network with viruses or publish company secrets? The key to managing these risks is a policy that defines acceptable Internet use and implementation of safeguards to ensure compliance with the policy. This paper describes the ...

Copyright SANS Institute
Author Retains Full Rights

AD

Managing Internet Use
Big Brother or Due Diligence?

Introduction 1
Internet Access Risk Assessment 1
Excessive Non-Business Use 1
Inappropriate Internet Use 1
Unauthorised Software 1
Language Issues 1
Unapproved/Unmanaged Connections 1
News, Chat and email 1
Policy Considerations 1
Privacy Issues 1
US Law 1
UK Law 1
Summary 1
References 1

Introduction

Internet access has become an established business tool, taken for granted along with email, telephone and facsimile. Like these other media, giving staff access to the Internet has risks – will they spend all day downloading porn or swapping chat messages with their friends? Will they infect the network with viruses or publish company secrets?

The key to managing these risks is a policy that defines acceptable Internet use and implementation of safeguards to ensure compliance with the policy. This paper describes the major risks of granting widespread Internet access along with suggestions to mitigate them. It also covers monitoring policies and the privacy issues that arise from monitoring Internet use.

Internet Access Risk Assessment

There are risks inherent in granting any group of users access to the Internet from work and it is irrelevant whether this is part of the workforce or the entire workforce.

A qualitative risk assessment is summarised in the table below. In this assessment Threat (potential cause), Vulnerability (weakness) and Impact (business outcome) are rated High (3 points), Medium (2 points) or Low (1 point) and the values multiplied together to give a risk score between 1 and 27.

Note that this assessment is of inherent risk and does not consider mitigating factors that a company may already have in place.

Threat (High, Med, Low)	**Vulnerability** (High, Med, Low)	**Impact** (High, Med, Low)	**Risk** (1-27)	**Mitigation**
Excessive Internet Use (H)	Inadequate reporting of use	Wasted time (M)	18	Acceptable Use Policy. Usage monitoring and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

	(H)			reporting
Excessive Internet Use (H)	Connection not authenticated (H)	Lack of accountability (H)	27	Require all connections to be authenticated

Inappropriate Internet Use (M)	Staff able to access such sites (M)	Can be sued for hostile workplace (M)	8	Acceptable Use Policy. Implement blocking capability. Disciplinary Process.
Unauthorised software (M)	Staff able to install software (L)	Local PC destabilised (L)	2	Policy Lock Down PC Audit
Unauthorised software (M)	Non-compliance with licenses (M)	Sued by vendor (H)	12	Policy Lock Down PC Audit Approved purchase route
Unauthorised software (M)	Virus/Trojan introduced (L)	Loss or disclosure of data (H)	6	Policy Lock Down PC Anti-virus software
Users don't speak English (M)	System messages in English (M)	Policy not followed because not understood (M)	8	Translate Policy Login banners in local language Error pages in local language
Users access inappropriate foreign sites (M)	Blocking lists UK/US centric (M)	Hostile workplace action (M)	8	Encourage vendors to assess non-UK/US sites Report such sites for inclusion in lists
Users connect standalone PC directly to Internet (H)	Information on PC inadequately protected (H)	Disclosure of data on PC, route to introduce Trojan. (M)	18	Acceptable Use Policy Encrypt Hard Disk Secure OS Personal Firewall Education
Users connect networked PC directly to Internet (H)	Breach firewall (H)	Disclosure of data on network, route to introduce Trojan. (H)	27	Acceptable Use Policy Secure OS Education War dialing Network segregation
Social chat/email use (H)	Can't distinguish from work use (M)	Wasted Time (M)	12	Acceptable Use Policy Education Usage Reporting Block IRC ports & chat sites
Social chat/email use (H)	Can't distinguish from work use (M)	Misrepresent company (H)	18	Acceptable Use Policy Education Disclaimer messages
Social chat/email use (H)	Harvesting of email addresses (H)	Spam email Abusive messages (L)	9	Education

Table 1: Qualitative Assessment Of Risks Intrinsic To Internet Access

The major risks are considered in more detail in the following narrative.

Excessive Non-Business Use

Excessive non-business related Internet use is a risk both in terms of lost productivity and in competition for infrastructure resources for legitimate business use. Various surveys[i] have estimated the time spent on non-business browsing by US and UK workers to average 30 to 60 minutes a day. Surfcontrol, an IT vendor selling Internet

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

monitoring and blocking software, estimate the lost productivity of a pharmaceutical industry worker who spends one hour a day on non-business use as $43,000 a year[ii] If this figure is even remotely accurate it totally outweighs the cost of "wasted" infrastructure in providing non-business Internet access and provides a very good incentive to adopt measures to limit such use.

Our experience is similar and analysis of usage logs indicates that 50-70% of hits are against non-work related categories of web sites. Even though blocking is in place to prevent access to inappropriate categories such as sex, illegal drugs, race hate etc. there are still plenty of compelling sites available on which employees can spend time.

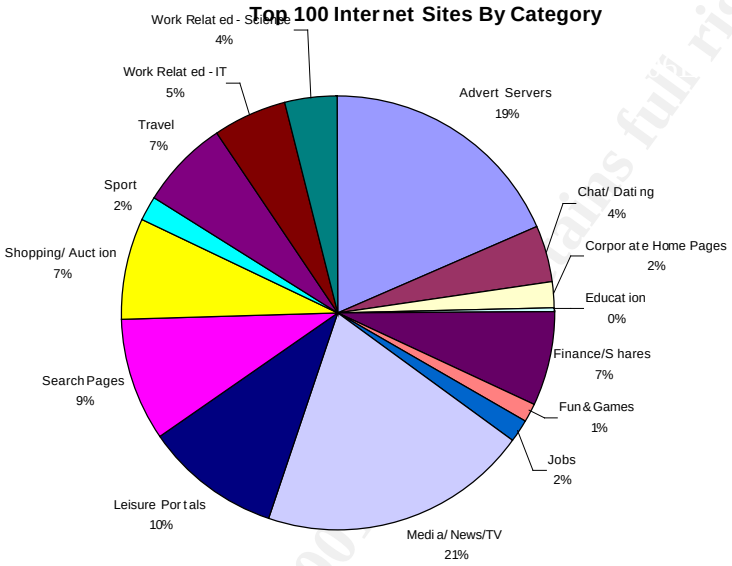

Chart 1:Hits against Top 100 web sites, grouped by category. These sites represented 24% of the total daily traffic.

The time spent browsing by the most active 100 users on this date ranged from 1:08 hours to 15:46 hours with a median of 05:21 hours. These users represented 14% of the total daily activity.

It can be argued that these statistics are deceptive because apparent usage can be pushed up by web pages that autorefresh every few minutes, such as stock tickers, and users may be doing their daily work while running a browser in the background. Also, some of the most popular web sites contain both work-related and non-business information (e.g. news sites) however when the most popular sites visited by the most active users are examined there is rarely a correlation between the individual's role and the sites they read – for example, the top visitors to finance sites tend to be IT contractors checking their stock portfolio.

It is apparent that there are many users who spend several hours a week on non-work related Internet browsing, with share tracking and dealing, reading news, shopping and travel being the favoured occupations. The challenge for companies is to keep such use within acceptable limits.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Mitigation

Ultimately the effective supervision of staff, to prevent excessive Internet use, is a local management responsibility. Extensive blocking lists will not deter hardened "cyberslackers" who will just seek out ever more obscure sites on which to waste time. Widespread blocking will also penalise responsible Internet users who wish to visit a non-work-related site for a short time, perhaps to check a sport score.

It can be difficult for line management to track the extent to which their staff are using the Internet – is the employee starting intently at his screen browsing or working? Some companies, such as Hewlett Packard, generate weekly reports listing the total Internet use for each employee, without giving details of what they are looking at. If one member of a team spends a disproportionate time online the manager can then take action. The return on investment of developing such a reporting system is high, given the infrastructure capacity and productivity recovered by deterring excessive personal use.

Hewlett Packard has developed a usage monitor suite of tools that tracks Internet use and can be used to report and even charge for total use. Although these tools are intended primarily for ISPs, they could also be adopted by large corporates with a complex infrastructure.[iii] In less complex environments log reporting tools such as NetIQ's WebTrends can be used to generate reports of sites visited by individuals and time spent online[iv].

In cases where staff do not need Internet access to do their job use of Internet kiosks or cyber cafes can be effective in limiting excessive use. The employee can be seen to be away from his usual workplace so peer and management pressure will be brought to bear if the time away is excessive. Dedicated clients also limit the risk of downloaded malware spreading to the wider network.

Inappropriate Internet Use

This risk is primarily of employees visiting sites with objectionable content. Cultural acceptance of content will vary between regions, for example displaying a "topless" calendar that would be unremarkable in Europe, could lead to termination of employment in the US and even more drastic sanctions in strict Muslim countries.

> *The Web@Work Survey 2001 reveals that British employers are five times more likely to take disciplinary action than Italian employers - and two-and-a-half times more likely to take action than their French or German counterparts.* [v]

Internet browsing is generally a more private activity than displaying a calendar so the impact of an individual browsing an adult site is relatively low. The serious impact comes if they expose other members of staff to the material, whether deliberately or accidentally. This can be construed as creating a hostile work environment and hence as sexual harassment in the workplace

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

> *Employers must consider that sexual harassment charges can also arise from obscene and harassing uses of the company's e-mail, intranet or Internet systems. The Internet is a gateway to an immense library of pornography, and pornographic sites are an enormously popular destination for many Internet visitors. Because employees who view such material in the workplace may be creating a hostile work environment for others, such activity must be strictly prohibited.*[vi]

A recent case relates to the Minnesota public library system where employees of the library were exposed to sexually explicit images

> *The Equal Employment Opportunity Commission (EEOC) ruled in late May that the library, by exposing its staff to sexually explicit images on unrestricted computer terminals, subjected the employees to a hostile work environment. Preliminary estimates from the EEOC indicate the library could ultimately be liable for more than $1 million in settlements fees*[vii]

Mitigation

Mitigation against the risks of inappropriate browsing and a sexual harassment action has three elements

1. An appropriate use policy that has been communicated to all employees.
2. A URL blocking capability that protects users from accidentally straying on to inappropriate sites, and makes it harder for users to deliberately access inappropriate sites.
3. An investigation and disciplinary process so that offenders are dealt with consistently.

Ideally all three elements should be covered but in some cases, such of that of the public library above, most of the effort needs to be put into monitoring and blocking technologies because there are few effective sanctions against a customer who ignores the rules.

It is important to note that these actions do not guarantee that inappropriate content will never be accessed. Rather they create a barrier to inappropriate use such that the company can demonstrate due diligence (i.e. that it has taken all reasonable steps) in protecting its employees.

Unauthorised Software

Employees with Internet access are able to download software. This could be commercial software or shareware that is not part of the standard desktop, but could also be Trojans and viruses. Cosmetic “skins” to customise the appearance of applications such as browser toolbars are increasingly popular. The risk of obtaining and installing software is that it may compromise the integrity of standard desktop software, particularly of validated systems. There are well documented cases of software being infected with viruses, for example a recent service patch from Microsoft was infected with the Funlove virus.[viii]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

There is also the risk of non-compliance with licensing terms, for example commercial use of a product that is only free for personal use. Much software is distributed through vendor web sites and the temptation is for users to download the evaluation version and only purchase the product through official channels if it stops working.

The impact of unauthorised software will vary depending on the sensitivity of the system on which it is installed. Some users who evaluate new software are highly IT literate and self-supporting, undertaking such activities in the course of their work and can provide great benefit to a company. Others work on strictly controlled PCs that are part of formally defined and validated systems. Installation of unauthorised software on such a PC compromises the entire system.

Mitigation

The computing acceptable use policy should define the routes by which users can obtain software and emphasise that bypassing these routes is not permitted. In the increasing number of cases where the vendor's distribution channel is the Internet, the software should be downloaded by IT support staff and tested on a reference PC before being installed, by them, on the user's desktop.

It is important that virus scanning of software is performed as it is downloaded from the Internet. It is likely that software will be installed/run as soon as it is downloaded so any hostile payload will be triggered before a desktop virus scan next runs. This emphasises the need to test the software on a quarantine PC before exposing it to the production environment

Tools such as Microsoft's Systems Management Server can automatically perform regular audit/scanning of PCs for unauthorised software. The sanctions in such cases can range from removing the software, to reinstalling the desktop or disciplinary action.

Highly sensitive PCs should be locked down so that they don't have Internet access and their users do not have sufficient rights to install unauthorised software, instead users can access the Internet from dedicated PCs or kiosks.

Language Issues

It is important to remember that many Internet users in a multinational company will not have English as their first language. Most staff in professional roles are likely to speak and read English but as Internet access becomes more pervasive the proportion of non-English speaking users will increase. This has two implications:

Users may not be able to understand login banners, acceptable use pages, error messages etc displayed by the Internet connection. It will be difficult to enforce messages that they cannot understand.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Users may access foreign language sites that are inappropriate but IT Security will not understand them. Blocking software tends to be focussed on English language sites.

Impact is likely to be low because acceptable use can be communicated by local staff who speak the language. In the case of inappropriate sites one can normally draw conclusions from the pictures without needing to speak the language.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Mitigation

Acceptable use policy, as a minimum, must be available in the local language of the individuals who are being asked to abide by it. Local IT staff should be encouraged to translate the English language version of the policy and then communicate it to their colleagues.

Vendors of blocking software should be encouraged to review non-English sites and there should be an official route for security managers to report such inappropriate sites back to the vendors for inclusion in their block lists.

Unapproved/Unmanaged Connections

Home use of the Internet is now widespread and many staff are perfectly capable of setting up their own Internet connection through a modem to an Internet Service Provider. Having gained skills and performance expectations at home, they may consider that dial-up connections offer better performance than the official gateway and without the constraints that the blocking software or firewall imposes.

Most laptops have modems that are used to dial in to the company network. It is likely that when staff are traveling the laptop is the only client available on which to access their personal email and Internet services. Consequently it is understandable that users will be tempted to configure their laptop to dial their home ISP.

Although such “standalone” use does not directly compromise the company infrastructure it does risk exposing any information on the PC to the Internet. As well as sensitive business information, access to the PC may also reveal information about infrastructure systems such as dial in numbers, configuration settings and passwords that a hacker could use in a subsequent attack. A Trojan or virus could also be installed on the PC while connected to the Internet that triggers when next connected to a network. This is a particular risk if the firewall offers a default route to the Internet that a Trojan can utilize.

If the dial up Internet connection does happen to be used while the PC is connected to the network then the potential impact is very much higher because the connection risks disclosing confidential information anywhere on the network to the Internet and allows hackers to bypass the company firewalls.

Many hotels now offer high speed access to the Internet at a fixed price per day. Typically this is achieved by connecting the laptop to the hotel network, which provides a shared high speed Internet connection to all guests. The risks of such a connection are similar to dialing the Internet – data on the PC is unprotected from Internet users. In addition other laptops connected to the hotel network, in other rooms, will be able to monitor the passing network traffic and can gain access to the PC hard drive with relative ease.

"Bluetooth" wireless connections in other public places, such as airports also risk the information on the client being exposed to third parties.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Mitigation

Users should be educated to be aware that the most secure way for them to connect to the Internet is through the firewall-protected company gateways. It must be highlighted that these gateways are essential in protecting the company from the risk of disclosure of confidential information and viruses.

The performance of approved Internet connections should be at least as good as that of a dial up connection, removing the temptation to use an independent connection for performance reasons.

PCs should be audited for the existence of non-approved dial up connection settings and software, with enforcement action being taken if necessary. Desktop management tools such as Microsoft SMS and HP Openview can create inventories of PC configurations.

Incidental personal use of the Internet through firewalls and permanent connections should be tolerated, if not encouraged, as this is the route that allows risks to be managed most effectively. However the personal use should be monitored carefully to ensure that is it not excessive or inappropriate.

News, Chat and email

Possibly the greatest business impact of chat and personal email is the distraction it causes. Real-time chat is particularly disruptive because it requires the users' immediate and ongoing attention. The immediacy of the medium, particularly as discussion becomes heated, can result in messages being posted without due consideration. These messages can then be construed as the individual speaking on behalf of the company when in fact they are giving a personal opinion. The company may be held accountable for such statements.

Names and email addresses can also be harvested from newsgroups and web pages, for example by using a search engine to search on the domain name. This can give rise to "spam" advertising but can also make staff the victim of more aggressively targeted email, particularly if they work for a company whose activities are controversial. In the UK and US staff and customers of Huntingdon Research Limited have been targeted in this way by animal rights activists. Such cyber-activism is becoming increasingly sophisticated with advice being given on how to evade email filters to make sure the message gets through.[ix]

Online databases such as www.192.com, which contains the UK electoral roll, make it easy to find an individual's home address based on their name and a rough location, such as the place they work. Thus an apparently harmless posting to a hobby newsgroup can lead to direct action at an individual's home.

Personal email downloaded by direct connection to ISPs and web-based mail systems (e.g. Hotmail) may also bypass attachment and content monitoring systems that are in

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

place on official Internet connections. This is another route by which Trojans and viruses can enter a company even when it virus checks its official email.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Mitigation

As with excessive browsing, effective management supervision is essential to limit the amount of time spent in non-work related communications. Policy highlights and education reinforces the risks of thoughtless message posting. Disclaimers stating that the views represented are personal opinions are of limited effectiveness in limiting liability when a message appears "from" a company employee. They are also difficult to engineer into real-time chat sessions.

There is a strong case to block access to chat and web-based email sites and most blocking software maintains a list of such sites. Similarly NNTP newsgroups (port 119) and Internet Relay Chat[x] (ports 531 & 6667) can be blocked at the firewall.

Users should be encouraged to protect their electronic identity and not post their email address indiscriminately on the Internet. Once an email address has been published it is impossible to remove and while generic spam messages sent to a wide distribution can be filtered reasonably effectively it is difficult to protect staff from offensive messages that are sent to them personally. In such circumstances the only resort is to change the email address.

Policy Considerations

Guidelines for creating an IT acceptable use policy are widely published on SANS[xi] and other web sites[xii]. The majority of companies recognise that a certain amount of personal Internet use is acceptable and can be in the company's interest – for example by allowing an employee to shop online rather than leaving work early to shop.

Measuring compliance with policy has been less well covered. Companies could consider implementing the following steps to ensure that employees' Internet use is acceptable.

Authentication
If Internet access is anonymous then it is difficult to track activity, all the logs will contain is the client IP address and this may be dynamically allocated. Having the client authenticate with the Internet gateway ensures that usage is assigned to individual user IDs. It also provides the opportunity to display an acceptable use banner.

Logging
Usage logs may be created by firewall and proxy servers. These will contain User ID, Client IP, URL requested and time stamp. Logs should be regularly reviewed to detect inappropriate use.

URL Blocking
Blocking software is very effective in restricting access to categories of web site that have been determined to be inappropriate. Many of the products will add a category code to log files for blocked sites. This makes it easy to filter a log and extract

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

attempts to access blocked sites. Given the low cost of blocking software, typically $10 a seat, it would be difficult for a company to defend a hostile workplace action unless it had implemented blocking.

Reporting
Usage reporting should be automated using the capabilities of the blocking software, with reporting tools such as WebTrends or with custom scripts. Care should be taken when reporting individuals' usage as this risks infringing their privacy. Privacy issues are considered later.

Investigation Of Inappropriate Use
IT Security should avoid becoming the moral guardians of the company. Inappropriate use is primarily a line management issue so any investigation should be managed by Human Resources departments, with IT security staff providing technical assistance. Policy should describe an escalation process by which incidents can be handed off from IT to HR and on to corporate security or even the police if necessary.

Data Retention
Companies should define a process to archive or dispose of log files. HR should retain any data that has been used as part of a disciplinary process, with other records relating to the case.

Privacy Issues

Any monitoring and reporting of Internet use risks that an individual's privacy may be compromised. The legal right to privacy may vary between countries but in most cases employees will have an expectation of privacy – albeit misguided. To give a concrete example, a female member of staff could be highly embarrassed should her browsing of www.abortionhelp.co.uk be publicised in usage reports. Consequently the acceptable use policy should make it clear that use may be monitored and staff using company assets have no automatic right to privacy.

US Law

There is little legal foundation in the US to protect individuals' privacy.

> *Since the employer owns the computer network and the terminals, he or she is free to use them to monitor employees.*[xiii]

Although the Electronic Communications Privacy Act (ECPA) generally prevents employers from monitoring communications it does support an employer's right to monitor stored communications, such as voicemail. An employer can monitor log files of Internet access in the same way that they can monitor phone logs to track personal use.

The main requirement of the ECPA is that employees must give their consent to monitoring. The recently introduced *"Notice of Electronic Monitoring Act"* requires

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

that employers notify staff of their monitoring policy on hiring and annually thereafter.

> *"If an employer electronically monitors an employee without giving the required notice, an employee may sue for civil damages. Compensatory damages are capped at $5000, and total damages are capped at $20,000. In a case where many employees are affected, per incident damages are capped at $500,000,"* [xiv]

Conversely, there is a requirement on employers to take steps to protect their staff from a hostile workplace.

> *"[The Supreme Court requires that] companies must take reasonable steps to prevent as well as quickly correct any hostile environment or sexual harassment behaviors as they occur. It can be interpreted that if there are reasonable technologies to able to prevent this from ever happening, companies must take those steps."*[xv]

The conclusion is that US law requires companies to implement processes, such as monitoring and blocking, to protect their staff and staff should have no expectation of privacy providing they have been informed of the monitoring. A wide-ranging review of employer monitoring published by the Privacy Foundation confirms this view

> *"A key question implied, but not addressed, by this research report is whether employers are giving employees sufficient notice of continuous Internet and e-mail monitoring. Because companies can use (or be seen as using) employee-monitoring logs as a kind of "wishing well" to justify actions against employees, including dismissals and layoffs, employers would be well advised to disclose to employees what is being monitored and why."*[xvi]

UK Law

In the UK monitoring of Internet activity is constrained by three acts; the Data Protection Act 1998, the Regulation of Investigatory Powers Act, 2000 and the Human Rights Act, 1998. The Human Rights Act is the UK implementation of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which is binding on all members of the Council of Europe.

The Data Protection Act governs the collection and use of personal data. In short, a company is only able to collect the data for which it has registered and only allowed to use that information for the purposes outlined in its registration. Individuals have the right to examine and correct the information that is held about them.

The Human Rights Act gives employees a number of rights including the right to respect for privacy and family life, home and correspondence and also the right to freedom of expression. In the context of employment law the rights can be qualified if an employer is able to demonstrate that measures must be taken to protect the rights of others.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Regulation of Investigatory Powers Act updated the law governing interception and monitoring of communications. The RIP act has been implemented as a series of regulations and codes of practise. The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations provide that

> *"employers retain the right to carry out monitoring despite the fact that employee has not given their express consent, if the monitoring is required to carry out the following:*
>
> - *Recording evidence of business transactions*
> - *Ensuring compliance with regulatory or self-regulatory guidelines*
> - *Maintaining the effective operation of the employer's systems (e.g. preventing viruses)*
> - *Preventing or detecting criminal activity*
> - *Preventing the unauthorised use of the telephone/email system – i.e. ensuring the employee does not breach the company's email or telephone policies*
>
> *Nonetheless, the Regulations provide that it will be necessary for employers to take reasonable steps to inform employees that their communications might be intercepted.*[xvii]

As with the US, UK law allows for monitoring Internet use but the employer is much better placed to enforce acceptable use policy if they make it clear what activity is being monitored and why.

The Data Protection Commissioner has issued a draft code of practice that includes the following advice

> *Unless such monitoring would be ineffective and the circumstances justify the additional intrusion:-*
>
> - *limit monitoring to traffic data rather than the contents of communications;*
> - *undertake spot checks or audit rather than continuous monitoring;*
> - *as far as possible, automate the monitoring so as to reduce the extent to which extraneous information is made available to any person other than the parties to a communication;*
> - *target monitoring on areas of highest risk*[xviii]

This code of practice is in direct conflict with the Regulation of Investigatory Powers Act and these inconsistencies are still being hotly debated.

Summary

As companies become aware of the amount of time employees spend browsing the Web, attention is moving from inappropriate use to excessive use. Monitoring and blocking software is undergoing huge growth as vendors focus on the issue to raise awareness and drive sales. At the same time there is a backlash from the media and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

employee advocacy groups claiming that any monitoring is an infringement of privacy and giving advice on how to escape detection.

Employees may have an expectation of privacy and be sensitive to "Big Brother watching them" but should be educated that they have no legal right to privacy when using company systems for personal use.
Gartner put this very succinctly:

> *Enterprises have to formulate sensible policies to balance employee privacy with the need to reduce their own legal exposure. However, this issue should not prevent enterprises from allowing some personal use of their IT systems.*[xix]

Companies are embracing the opportunities afforded by the Internet and granting access to an increasing proportion of their employees. This entails a number of inherent risks that can be mitigated by an effective Internet Acceptable Use Policy supported by effective processes to ensure that the policy is followed and an investigatory and disciplinary process if it isn't.

The key learning from this evidence is that we must have a policy setting out what use of the Internet is acceptable. This policy must be conveyed to all staff and they must understand that by following it they are protecting both themselves and the business. The weakest link in any IT Security process is the people involved. Once staff are educated and motivated to follow policy, implementing technical safeguards becomes much easier.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

[i] *"Results Of Vault Survey Of Internet Use In The Workplace"*, Vault, 2000, URL: http://www.vault.com/surveys/internetuse2000/index2000.jsp (July 17, 2001)

[ii] *"The Cost of Non-Business Browsing"*, Surfcontrol plc, 2000, URL: http://www.surfcontrol.com/news/white_papers/pdfs/SC_Cost_of_Browsing.pdf (July 17, 2001)

[iii] *"Managing Service Usage Data For Strategic Advantage"*, Hewlett Packard Company, April 27, 1999, URL: http://www.hp.com/communications/usage/infolibrary/siuwp2.html (July 17, 2001)

[iv] *"Firewall Suite"*, WebTrends, 2000, URL: http://www.webtrends.com/products/firewall/default.htm (July 17, 2001)

[v] Richardson, Tim. *"'Cyberslackers' are curse of workplace"*, The Register, 19 April 2001, URL: http://www.theregister.co.uk/content/archive/18378.html (July 17, 2001)

[vi] Townshend, Anthony M *et al*, *"Danger On The Desktop"*, HR Magazine, January 1997, URL: http://www.shrm.org/hrmagazine/articles/default.asp?page=1097INT.HTM (July 17, 2001)

[vii] *"Recent Equal Employment Opportunity Commission Ruling Against Minnesota Library System Has Many Companies Taking Closer Look at Merits of Internet Filtering"*, PR Newswire, June 20, 2001, URL: http://www.corporate-ir.net/ireye/ir_site.zhtml?ticker=NTWO&script=410&layout=-6&item_id=184612 (July 17, 2001)

[viii] *"Information About Virus-Infected Hotfixes"*, Microsoft TechNet, April 27, 2001, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/topics/vihotfix.asp (July 17, 2001)

[ix] *"How To Outwit The Email Filter That The Bank Of New York Put Up"*, SHAC USA, July 6, 2001, URL: http://www.shacusa.net/news/07-08-01.html (July 17, 2001)

[x] *"Internet Relay Chat Help Archive"*, 2001, URL: http://www.irchelp.org/ (July 17, 2001)

[xi] *"Model Security Policies"*, SANS Institute, 1999, URL: http://www.sans.org/newlook/resources/policies/policies.htm (July 17, 2001)

[xii] *"The Guide To Developing Your Company's Internet Acceptable Use Policy"*, SurfControl plc, April 2001, URL: http://www.surfcontrol.com/resources/business/acceptable_use_policy/aupuk_0401.pdf (July 17, 2001)

[xiii] *"Employee Monitoring: Is There Privacy in the Workplace?"*, Privacy Rights Clearinghouse, April 2001, URL: http://www.privacyrights.org/fs/fs7-work.htm (July 17, 2001)

[xiv] *"Legislation Targets Big Brother"*, PC World, July 24, 2000, URL: http://www.pcworld.com/news/article/0,aid,17795,00.asp (July 17, 2001)

[xv] Chen, H. *"Internet Use Survey 2000 -- Trends and Surprises in Workplace Web Use"*, Vault, September 1, 2000, URL: http://www.vault.com/nr/main_article_detail.jsp?article_id=19331&listelement=2&cat_id=0&ht_type=5 (July 17, 2001)

[xvi] Schulman, A. *"The Extent of Systematic Monitoring of Employee E-mail and Internet Use"*, The Privacy Foundation, July 9, 2001, URL: http://www.privacyfoundation.org/workplace/technology/extent.asp (July 17, 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[xvii] Nickson, S in *"The Guide To Developing Your Company's Internet Acceptable Use Policy"*, *Ibid*

[xviii] *"Use of personal data in employer/employee relationships"*, Data Protection Commissioner, October 2000, URL: http://wood.ccta.gov.uk/dpr/dpdoc.nsf (July 17, 2001)

[xix] Gassman, W, *"Allowing Personal Use of IT Systems May Even Benefit the Enterprise"* , Gartner, May 23, 2001, URL: http://www3.gartner.com/DisplayDocument?id=330381 (July 17, 2001)

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced