



Guide to Web Access Management

CONTENTS

A growing problem for businesses and public bodies alike	3
How do you know you have a problem?	5
How big is the problem?	6
What exactly are the problems?	8
Whose problem is it?	11
A web access and use policy	13
How do we enforce the policy?	16
The technology options	19
Conclusions	24
Appendices	25
Contributors	26

A growing problem for businesses and public bodies alike

The Internet – specifically the World Wide Web – is a very valuable vehicle for research, learning, marketing, and transacting business. But it is also a source of material that it is inappropriate for staff to access – such as gambling, pornography, or violence. Even web sites that are not offensive may have a significant adverse effect on staff productivity e.g. sport, gossip, and chat-rooms. Recent research¹ suggests that a typical company of 1000 employees can lose up to £2.5m a year through non-business use of the Internet. Also, such use absorbs valuable IT resources and means more costs are incurred in additional IT and network capacity.

Apart from the financial aspect, the impact on H-R policies and people management has an ever-higher profile. Increasingly, Internet abuse features in the top reasons for disciplinary action or dismissals.² The Information Commission recognises an employer's right to protect their business systems from abuse, but stresses the need for balance between that protection and intrusion into an individual's privacy. The Information Commissioner's draft Code of Practice³ permits monitoring of employee's use of the Internet, but recommends that such monitoring should aim to prevent rather than just to detect and penalise misuse.

In many organisations, however, a “blanket ban” on access to the WWW, or even on all sites other than approved ones, may be too restrictive. Certain departments may have legitimate business reasons for accessing sites that are “off-limits” to the rest of the company. For example, only Purchasing Dept. may be allowed access to on-line trading sites. Equally, employees may be allowed to access, for example, sports sites outwith normal working hours.

In all cases, it's now important that there is a clear company policy – an Internet Access Policy – that is both communicated and enforced. Such an approach contributes to maintaining good employee relations and to protecting

the company's assets, not least its reputation – a key concern of top management. Such technology policies must also refer to and be enforced by a companies disciplinary and HR policies. In order for an Internet Access Policy to be useful it must be able to be enforced by HR or management.

Officers/directors of any organisation are responsible for the use of resources in that organisation. If the IT network is used to access and distribute offensive material those officers can be held legally responsible.⁴ Responsibility for setting up and monitoring the policy often ends up on the IT manager's desk, because it's perceived as a technical problem. Equally, any exposure from not having an effective system – should it occur – may also end up on the IT manager's desk! The policy is better owned and managed by H-R; the implementation and monitoring managed by IT. Whoever has responsibility in an organisation, prevention is essential – reacting after an “incident” may be more costly than a measure of prevention.

IT technologies can provide excellent tools to implement and monitor a policy. Such technology comes in many guises and with varied scopes and capabilities. This paper will explore these, but will also set them into the context of a proper management system that covers the organisation-wide implications of Web Access Management.

-
- 1 Chartered Institute of Personnel and Development, Internet and e-mail policies, March 2000 / Nov 2001
 - 2 Article in “Personnel Today”, 10 September 2002.
 - 3 Information Commission's draft Code of Practice.
 - 4 Chartered Institute of Personnel and Development, Internet and e-mail policies, March 2000 / Nov 2001

How do you know you have a problem?

At worst, when it becomes public and you read about it! This is particularly true where “vulnerable” sections of society (e.g. children) are exposed to offensive material. But the nature of the problem is such that often it goes unnoticed, or ignored, or becomes “acceptable” because no action is taken to prevent it. This does not apply just to the most obvious forms of Internet abuse, such as pornography, but to the insidious waste of time and resources through non-productive surfing or game playing. Because such use is made up of lots of relatively small and intermittent cases, it is very difficult to detect through normal management activities.

Another manifestation is when your IT department try to diagnose problems on PCs and discover that unauthorised programs or incompatible versions have been downloaded from the Internet. Maintaining control over the software running on PCs is one of the growing headaches for IT managers. One potential exposure in this area is the increased likelihood of contravening software licence terms.

For those cases involving offensive material, the most likely way to find out is when staff complain of “harassment” and you have a personnel issue to handle.

How big is the problem?

It’s big and getting bigger – in two ways. Firstly the scale; most organisations now provide widespread access to the Internet as a core aspect of their business. Secondly the profile; failure to control the use of such resources can leave top management exposed to legal action and can damage the organisation’s public image.

The scale is growing. According to IDC Research, around 30% of employees’ Internet access is not for business purposes. As each employee with Internet access now spends on average 6 hours a week on-line, this amounts to some 2 hours a week of non-productive time per employee. With anywhere near this level of “wasted” time, the financial business case for addressing the issue is strong in most organisations. The return on investment will exceed most Financial Director’s guideline “hurdle rates” for projects.

70% of accesses to WWW pornography sites occur during the period 9am – 5pm, suggesting that browsing from the workplace is very common. Similarly on-line gambling links now feature on many “main line” web sites – some 40% of on-line “Casinos” now advertise on such sites rather than, as previously, only on specialist gambling sites.

So how well recognised is the problem? A recent survey by Personnel Today and KLegal produced the following findings:

- 20 per cent of employers monitor Internet access on a daily basis
- More than 90 per cent comply with the Data Protection Act
- More than 20 per cent monitor weekly or monthly
- More than 90 per cent of organisations surveyed have guidelines on the use of the Internet at work and 93 per cent of these claim to communicate this policy to staff

What exactly are the problems?

- There were 358 disciplinary cases of Internet and e-mail abuse reported by the 212 organisations surveyed
- 53 per cent of respondents have some software preventing access to inappropriate websites
- 71 per cent have firewalls to block inappropriate e-mails
- 60 per cent of Internet-related dismissals and half of disciplinary cases involved distribution of pornography or sexually explicit material

1 The size and growth of the Web

The World Wide Web has millions of websites and thousands more are added daily. Internet pornography is one of the few online trading industries that is highly profitable. There is a “sub-www” of interlinked sites that purvey pornography in all its myriad forms. Accessing these sites can be deliberate, or – as is often the case initially – by accident. Staff can “trip over” these sites while searching for quite innocent, even if not strictly business-related, information.

2 Pornography

Accessing pornography sites at work can be easy and can sometimes be considered a “personal and private predilection” even if not one to boast about (usually.) But the next step is to download images onto a PC and to distribute them – either for “interest” or maliciously. The distribution is usually via e-mail attachments. Whilst this also (in most cases) uses the Internet as a distribution medium, it is not the same as accessing the WWW and the technology is not quite the same. However, the WWW is the source of nearly all such images and controlling the access to unsuitable WWW sites is likely to address most of the problem at source.

3 Gambling

Web-based gambling is as addictive as traditional gambling; in some ways more so as it’s so easy and can be done from the “comfort of your office.” Apart from the time wasting, the potential effects on staff well-being can be severe.

4 Surfing for interest/hobby updates

Examples are sporting news reports, film and TV features, and music. Again, whilst most of these are “innocent” and may be allowable either in small amounts or out of core work hours, they can occupy both staff time and resources – particularly if music or film “clips” are watched “live” or downloaded onto PCs.

5 Shopping

Checking travel times and booking tickets for travel or events is not too disruptive, but trawling the web for “today’s offer” on cut-price holidays or participating in on-line auctions can take up a lot of time and attention.

6 Chat-rooms are also addictive

These are the on-line equivalent of street corner gossip. Communication is interactive; messages flit back and forth between correspondents within minutes or seconds. The attractions of these chats between people – sometimes across continents – are seductive and very consuming of time and attention.

7 Downloading programs

This always brings exposures. It may be that the programs contain viruses or similar malicious code. Even if the program is “harmless” it may be incompatible with other business systems or may violate the technical standards that are in place to make systems maintenance simple. There is always the risk that the program’s licence terms are breached and the company is held responsible, not the employee. An employer is also vulnerable to accusations of copyright

infringement where employees are permitted unlimited access to the internet and in particular the ability to download articles and other materials. This would be an infringement under the Copyright, Designs and Patents Act 1988 and is something that employees are often unaware of.

The other side of the above problems is that in some cases there is a genuine business reason for access to such sites. Journalists do need to read news reports. Procurement departments do need to work with on-line purchasing sites. Health organisations do need to read about (some) sexual matters. What may be a problem in one situation may not be in another. As the problems are so intractable and particular to each organisation, the solutions are not so simple and universal either.

Whose problem is it?

Unfortunately, quite a few people's in any organisation. At first glance it's often thought of as a technical problem; in other words something to park on the IT Manager's desk. But that is a very simplistic view – as is increasingly echoed by IT managers! The issue at root is about the behaviour of staff at work and their use of business tools. That is the province of management – the line managers who are responsible for their staff's behaviour and effectiveness at work. In most cases, those line managers will look to Human Resources for guidance and support in communicating and enforcing company policy. Decisions on access to technology must be disseminated throughout the company and enforced by the appropriate personnel.

So it's H-R's problem then. Yes – fundamentally. But two other areas are also affected. Finance, who have to pay for the non-productive use of resources and of employees' time. And, not least, the chief executive, who will bear the brunt of any public exposure and the implications for the organisation's image.

There are clear legal implications for all of the directors / officers in the organisation. Employers could be responsible for their employees' activities when using the Internet and in order to avoid being held liable for employees' actions (such as obtaining or distributing illegal, pornographic, or racist material which might be offensive to colleagues) employers must be able to prove that they have a policy in place to prevent illegal actions and that appropriate steps are taken to enforce this policy. Also the viewing of pornography in the workplace has been held to be sexual harassment under the Sex Discrimination Act 1975.

So, back to IT for the enforcement? Partly. IT can set up controls to bar access to known sites (or those with obviously inappropriate content) and to monitor if, how, and by whom any of these are accessed. But the monitoring is one aspect only. The key is an integrated policy for using the Internet as one

of many business resources. The policy must be established and communicated and upheld – just like any other significant company policy.

A web access and use policy

OK, so we need one. What should it look like and how will I know we have got it right?

Like all company policies, the main things are that it is communicated effectively and understood and accepted as reasonable by all members of the organisation.

So the decisions to be made at the outset include:

- What topics do we wish to bar completely?
- What topics do we wish to bar in core work hours, but not outside those hours?
- What topics do we wish only some groups to access?
- Do we wish to allow personal use of the Internet and WWW – if so how much?
- Do we wish to monitor all accesses?
- Will we get reports with users identified or just statistics “company-wide” or by “user group”?
- If a user tries to access a prohibited site or download prohibited files, what action do you wish to take? Issue a warning message only, or note the details of the incident in reporting – either anonymously or with user identified?
- What sanctions will we impose on offenders, either “first time” or “persistent”?
- What feedback will we give to managers and staff on general or specific outcomes of the policy?
- How does this policy fit in with other related policies on e.g. passwords, confidentiality, e-mail, and copyright?

Depending on the answers to the above, you can frame your policy. Then comes the H-R / legal bit. Your policy should be communicated, formally, to every member of staff (and don't forget to include it in the induction process for new staff.) You should require them to acknowledge the policy – by signing an agreement to the policy. This agreement may include recognition and acceptance that Internet use will be monitored.

The policy must conform to several legal requirements, including (but probably not only):

- 1 The Data Protection Act. These requirements are covered well in The Information Commission's Code of Practice: Monitoring at work, an employer's guide. Amongst other recommendations, this Code of Practice recommends that employers carry out an “impact assessment” of any proposed monitoring. Such an assessment should consider:
 - The benefits that monitoring will bring to the organisation
 - The techniques that can be used and their relative advantages
 - Any adverse effects on staff as a result of the monitoring approach proposed, and
 - Whether equivalent or sufficient benefits can be obtained by an approach that has less impact on staff.
- 2 The Obscene Publications Acts, 1959 and 1964.
- 3 The Computer Misuse Act 1990
- 4 The Human Rights Act 1998
- 5 The Trade Marks Act 1994

How do we enforce the policy?

6 The Protection of Children Act 1978

7 The Copyright, Designs and Patents Act 1988

8 The Regulation of Investigatory Powers Act 2000

Do you have a good policy? Only you can really judge. Will it work in your organisation? Will it get the support of staff? Can you implement it at reasonable cost and enforce it with confidence?

The Appendices contain a reference to existing policies that may be a useful guide.

There are two elements that you should consider: technical capabilities and management ones. The latter are, in essence, common sense and good practice in any aspect of people management:

- Make it clear what is expected
- Show that you mean it
- Lead by example
- Address issues quickly, and fairly and in accordance with the appropriate company policies
- Learn from experiences

The technical capabilities, by contrast, are evolving all the time and are providing ever more flexible tools for implementing and enforcing a policy. There are several technical approaches, but they each cover some or all of:

- Blocking access to all or specified parts of the WWW
- Allowing access only to specified parts of the WWW (sometimes called a “walled garden” approach)
- Blocking (selectively) access to sites that are recognised to have particular characteristics
- Blocking access to individual web pages that are recognised to have particular types of content
- Prohibiting downloading of specified file types.

The next chapter covers the pros and cons of each of the above approaches.

Whichever approach is adopted, the complementary aspect is reporting on

what is happening. The monitoring tools can not only block/restrict access, but can usually identify who is doing/attempting the access (or at least, which PC is being used.) The more sophisticated can associate the access with the password and ID of the user, which should be sufficient to identify the user – unless IDs and passwords are being shared.

Once the monitoring is set up, acting on the reporting is the responsibility of H-R and line management and must reflect the policy that has been agreed.

Note that “accidental” or “casual” misuse will usually be deterred by a simple warning message. For example: “You have requested access to a web site that is not allowed under the company’s Internet Use Policy. If you need to access this site for business purposes, please arrange with your manager to have the restriction changed.” If the restriction is potentially incorrect, then it is management’s responsibility to assess this and initiate a change. In any case the user has been reminded both of the policy and that it is being monitored. This is the ideal scenario – prevention is the priority and a low-key response is adequate.

More determined users (or those whose ingenuity is challenged by the policy) might persist in trying to find alternative routes to the sites. A good web monitor will catch these attempts, too, and will build up the statistics for management to take action. A “medium-key” response is to communicate generally the overall statistics to remind everyone of the policy and as a “shot across the bows” to those generating them! Only when persistent or extremely serious (and maybe on occasion successful, because no system is yet 100% watertight) breaches of the policy are identified may a “high-key” and personalised response be required. Where the borders are between these various responses will depend on your organisation and your policy.

Employees’ actions (such as obtaining or distributing illegal, pornographic,

or racist material which might be offensive to colleagues) employers must be able to prove that they have a policy in place to prevent illegal actions and that appropriate steps are taken to enforce this policy. Also the viewing of pornography in the workplace has been held to be sexual harassment under the Sex Discrimination Act 1975.

So, back to IT for the enforcement? Partly. IT can set up controls to bar access to known sites (or those with obviously inappropriate content) and to monitor if, how, and by whom any of these are accessed. But the monitoring is one aspect only. The key is an integrated policy for using the Internet as one of many business resources. The policy must be established and communicated and upheld – just like any other significant company policy.

The technology options

1 Firewalls

These are devices (or sometimes software for individual PCs) that sit in the local network between the LAN and the outside world. They stop unauthorised access from the outside world into your systems. They are a defence against hackers and against specified types of data being transmitted into your system. They do not, and are not designed to, prevent access to outside data sources from within your organisation.

2 URL filtering programs

These are licensed programs that reside on your servers and which check the addresses (URLs) of web sites that users are accessing. They contain (either within themselves or via a link to a “master” server) a database of web sites classified according to their content – “gambling, sport, shopping” etc.) When a web site is requested, the program checks the classification against the authorisation accorded the user and either allows or refuses the access request, and logs the attempt.

These programs are effective in:

- a Demonstrating that monitoring is happening
- b Preventing access to known sites (i.e. URLs that have standard classifications and are restricted by the policy)
- c Allowing an organisation to set up “white lists” of sites that are allowed, despite any standard classification. Similarly local “black lists” can be set up.
- d Reporting on allowed / disallowed access requests

They are less effective in:

- e Trapping sites that have not yet been classified
- f Catching personal sites such as “Yahoo Groups” some of which contain extremely offensive material, without blocking the whole of such sites.

3 Image scanning programs

These programs work by analysing images for flesh tones. More sophisticated versions will also take into consideration the geometry of the images looking for key features that would imply offensive material. Image scanning technology is mainly used for processing e-mail attachments where the delays resulting from the relatively slow scanning operation does not cause a problem.

These programs are effective in:

- a Blocking explicitly pornographic images.
- b Being constantly up to date by virtue of their dynamic nature.

They are less effective in the following areas:

- c They concentrate on blocking pornography, so image analysis will not pick up violent or distasteful sites that do not have a high graphics content.
- d Because of the high processing overhead, the performance of the Internet connection can be severely impaired, especially on high-speed connections.
- e The images have to be downloaded before they are blocked. URL filtering blocks the actual request before the image is downloaded to the network.
- f Image scanning cannot recognise offensive text.

- g Image scanning can cause harmless images such as holiday photos etc. to be blocked.

4 Fingerprinting programs

Fingerprinting programs work by generating an electronic “fingerprint” for each image as it is downloaded. This electronic fingerprint is then compared against a previously generated finger print library and the image blocked if a match is found.

These programs are effective in:

- a Tracking the progress of known documents through a network.

They are less effective in:

- b Blocking new sites. Because the fingerprinting technology is based upon a fingerprint library, the database can never be completely up to date.
- c Stopping documents before they enter a network. Generally the software is deployed on all the machines in the network. By the time the finger printing technology has spotted the rogue file it has already breached the firewall and traversed the Local Area Network.

5 Page scanning programs/devices

Page scanning technology scans requested web pages looking for sequences of keywords. If certain keywords are found in the document it will be blocked. More sophisticated products build up a score of keywords and block the page based upon that score. A good page-scanning product should have a scoring system that accounts for the context in which a word is used, i.e. “breast cancer”

should not block a site, whilst “naked breasts” probably should.

These programs are effective in:

- a Blocking new sites as they are brought on line. The dynamic nature of the page scanning technology allows sites to be blocked the minute they come on line.

- b Monitoring chat sites for offensive messages

They are less effective in:

- c Blocking image-only sites.
- d Sites that use foreign character sets.
- e Business, news, and entertainment sites.

5 E-mail scanning programs

These programs check the content of e-mails and attachments to e-mails. There are several versions, similar to the web page image / text scanners described above.

These programs are effective in:

- a Stopping the proliferation of inappropriate materials that have already been imported, not only from the WWW
- b Discouraging inappropriate messages being sent

They are not effective in:

- c Preventing material being accessed or downloaded from the WWW

Conclusions

d Preventing non-productive web surfing.

So what? The most practical answer is a combination of the above, utilising the strengths of those approaches to address the issues most important to you. The set of functions that covers most of the common (and significant) exposures, with generally the least overheads is:

- A firewall
- A URL filter
- A web page content scanner, and
- An e-mail scanner.

Every organisation that provides employees with access to the WWW should assess the risks to those employees and the organisation of allowing un-fettered access. There are potential financial, personnel, legal, and image exposures if this is not done.

A well-communicated policy covering Internet Access is a sensible approach in all cases.

H-R is probably the best function to take responsibility for establishing and enforcing that policy because of the overview that they have of the company and its disciplinary policies. The IT department can help to implement and monitor the policy and there are now many tools to assist in this. But IT tools are most valuable in supporting the people-oriented aspects of the policy, not as an alternative.

Appendices

A Further reading / information / advice

- a Chartered Institute of Personnel and Development: Internet and e-mail policies – originally issued March 2000, minor revisions November 2001. See the “Quick Fax” series of documents at www.cipd.co.uk/Infosource.
- b “The Information Commission’s Code of Practice: Monitoring at work, an employer’s guide.” See: www.dataprotection.gov.uk/dpr/dpdoc.nsf/ “Drafts for consultation.”
- c Federation Against Software Theft. See www.FAST.org.uk
- d Packet Dynamics ltd. See www.bloxx.com

B Sample Web Access policies

There are many such policies available on the WWW.

One well-established policy from academia is the JANET Acceptable Use Policy at: www.ja.net/documents/use.htm

Contributors

Bloxx Ltd

Bloxx is a UK company founded in 1999, specialising in the manufacture of the Bloxx range of web filtering appliances. It has a successful track record of addressing the growing market for Internet Access Management systems.

McGrigor Donald