

Internal Audit Report

Internet Usage

WEST MIDLANDS FIRE SERVICE

Report No: FS119

Date Issued: 21 April 2009

Report Author: Tony Brown, IT Auditor

**Quality Review: Peter Farrow, Audit Services and Risk Management
Manager - Sandwell MBC**


Report Distribution:

Lynda Bateman – Treasurer

Alan Brandon - Director of Corporate Planning & Support

Contents:

- 1 Introduction**
- 2 Background**
- 3 Conclusion & Summary of Key Findings**
- 4 Findings & Recommendations**
- 5 Action Plan**



Sandwell Audit Services are pleased to be making a positive contribution to saving our rare and endangered species from extinction by sponsoring Tangra the Snow Leopard (pictured above) who is based at Dudley Zoo as part of the European Species Survival Programme. Snow leopards are found in the high mountains of Central Asia, specifically the Himalayas. They are powerful, agile animals, unfortunately they are also an endangered species as they live in a harsh and dangerous environment and are illegally hunted. The total population of the snow leopard is now in hundreds rather than thousands.

1 Introduction

At the request of the Treasurer we undertook a review of the practices and procedures in place over the use of the internet within the Fire Authority.

2 Background

As with most organisations, use of the internet has grown significantly over recent years. With nearly 4,000 users, ensuring that it is used productively, in accordance with local policies is a fundamental necessity. Since the previous audit of this service, significant investment has been made in installing automated tools (Websense) that control the content of websites that users can access. These produce an audit trail (log) of all internet activity, showing which sites were accessed, which has been blocked and what subjects users have searched for.

This audit concentrated on analysing a sample period of log entries in order to determine how well these controls were operating and generally, to identify whether there were any issues that management should be aware of / take further action on.

3 Conclusion and Summary of Key Findings

Taking account of the issues identified in this report, in our opinion the controls within the system, as currently laid down and operated, provide **limited assurance** that risks material to the achievement of the organisation's objectives for the system are adequately managed and controlled. We found:

- There was no effective formal Internet Usage Policy in force until November 2008.
- Administrator Alerts for potential misuse of the internet were not being investigated.
- A need to examine organisational policies regarding the use of social networking sites (ie. Facebook) and the installation of wallpaper images.
- Software used to block inappropriate sites appeared to work well.

From our review of internet logs covering a three month period (August to November 2008) we identified the following:

- No evidence of deliberate attempts to access pornographic material.
- Approximately one quarter of all Internet Accounts were not traceable to individuals - the Authority's Single Sign-on policy can present security and management difficulties.
- An undetected error meant that the log entries for nearly the whole of November 2008 were not recorded.

Acknowledgement

A number of staff gave their time and co-operation during the course of this review. We would like to record our thanks to all of the individuals concerned.

4 Findings and Recommendations

4.1 Policies & Procedures

Our previous internal audit report on Internet & Email services, issued in 2006 included the following recommendation:

"An appropriate Acceptable Use Policy to be fully implemented including suitable levels of promotion and availability of copies (printed / electronic)".

At that time management confirmed that this was ready for consultation and due to be implemented by December 2006. However, at the start of this review the policy had yet to be approved and issued. The Standing Order 1/20 – Acceptable Use of the Internet was subsequently issued on 21 November 2008. Therefore, there was no formal policy specifically covering internet use, in place until this date. A similar Standing Order 1/19 – E-mail Acceptable Use Policy was issued in July 2006 and did cover acceptable/unacceptable use of emails (including notification that monitoring would occur), however, email use is different to internet web browsing.

A statement is displayed upon the log-in screen of each PC stating *"Access to this system is restricted to authorised users only. It is only to be used for the business of the Authority in accordance with the Fairness & Equality & Use of ICT policies. By continuing you are indicating acceptance of these policies. For guidance please call xxxxxxxx"*. However, there were no specific policies with the titles quoted, and, as such, it is arguable that staff might reasonably not know what might be considered appropriate or not.

- 4.2** We were also able to confirm that full backup arrangements were in place for internet log files, in accordance with recognised good practice, normally enabling details to be examined for the previous 12 months.

In our previous report we also made a further recommendation:

"Consider the introduction of regular analysis of internet browser session log-files using automated tools".

This was agreed, with an implementation timescale of April 2007. However, no routine examination of internet logs has been undertaken and it was indicated that reports would only be generated if specifically requested in relation to a particular investigation. Though, obviously this would not be instigated based on the log details.

- 4.3** The Authority does not utilise specialist flesh-tone detection software to supplement their control systems. This software examines the content of image files to intelligently determine whether the subject matter may be pornographic. While it is not common-place to use such software, it can aid the interception of unsuitable material. While we have not recommended the utilisation of such software (as a result of the use of Websense), it may be something the Authority wishes to consider in the future.

- 4.4** We were able to confirm that there were no stand-alone PCs with direct internet access that did not go through the central gateway and control systems.
- 4.5** We also requested details on all IT equipment issued to the former Chief Fire Officer, along with details of their current location (as older equipment may have been reallocated to another officer, or, be redundant, awaiting disposal) in the event that this might be of interest in the current police investigation. From the information provided, it was evident that an older laptop, used between October 2006 and January 2008, was still on-site, awaiting disposal. Steps were taken to immediately secure this machine which was subsequently passed into the custody of WM Police.

Recommendation 1

The Authority should agree the scope, period and responsibility for a regular analysis of the internet logs. We would recommend that this be at least monthly and include:

- attempted access to adult material
- access to social networking sites (eg. Facebook)
- unexpected Out of Hours activity

Recommendation 2

All system generated Alerts should be promptly examined and appropriate action taken and documented.

4.6 Analysis of Websense Internet Log Files

The authority uses market-leading Websense software as a gateway for all internet access. Various levels of access are provided, with control down to individual users and sites. A comprehensive categorisation of sites is maintained by the software, allowing separate rules for example, for news sites, drugs, shopping, sport etc. By default, access to sites of a pornographic nature are blocked for all access levels.

All activity is recorded in continuous log files, showing the date & time, the particular user, the site accessed, the site category and whether this was allowed or blocked.

Full internet log details were requested for a three month period:

Number of user accounts	3938
Number of log entries	10,081,179
First log date	19 August 2008
Last log date	28 November 2008 **

** The log files omitted any entries between 28/10/08 and 26/11/08. It was reported that this was due to an error with the server that had gone unnoticed and that this situation had also occurred on a previous occasion when details were needed for possible disciplinary action.

Recommendation 3

The Websense Server Event logs should be examined on a daily basis and any corrective action taken as appropriate.

- 4.7** A number of tests were conducted on this data, to confirm it was reliable and to examine whether any areas of significant misuse could be identified. The conclusions of the analysis using IDEA software are presented below:

4.8 Test 1 Web Site Categories

We checked to ascertain if category descriptions (eg. sport, news, shopping etc.) met the actual URL/page content, as, if we were to rely on selections of categories for further analysis, we needed to be confident that they were correctly categorised. With very few exceptions, the categories were found to be correctly categorised. There were no instances found of adult related material being coded against more innocent categories.

4.9 Test 2 Were any sites not categorised?

With the continual expansion of the web, no one list can attempt to know about every site, and correctly categorise its content. It is therefore to be expected that a number of sites will be recorded as unknown. Websense gives these a Category 153 - "Miscellaneous - Uncategorized". It is possible that unsuitable sites could be accessed which, at that time, are uncategorised.

The log files show a very small number of entries for this category, however, there was no evidence of misuse / unsuitable sites, with this mainly relating to WMFS applications.

4.10 Test 3 Generic User Accounts

We checked if there were any generic accounts (as these are difficult to trace back to an individual, therefore misuse could be harder to prove) and if so, was there any evidence of these accounts accessing inappropriate sites?.

There were 1,143 accounts that did not meet the normal user-based account format, of these:

- 818 were simply machine (IP) addresses, open to any user of that machine.
- 198 were for the Watch eg. Station, Colour / Admin / Guest
- 26 were titled "ADM." followed by a persons name
- 4 were titled variously A077 CSV01-4, B017 CSV01-4, C087 CSV04, HQMR, ICE, LR, STUDENT1-9, USAR, Freelance1-2

- 13 accounts had 4 character non-descript names but the system did hold the officer's full Forename and Surname details
- Others generic accounts included Band, Benevolent Shop, Credit Union, Direction of Travel, Fire Control, Hot Strikes, Retired Firefighters, Sysdev Green, Temporary Buyer, Test User, Tiger2020, YFA West Bromwich, Techrescue.

An examination of usage logs for these accounts showed no discernable difference to usage by individually named accounts.

However, we did find within the data that a number of entries were for Facebook, revealing a potential further policy issue (paragraph 4.17 refers to this in more detail).

Our earlier audit report issued in May 2006 made the following recommendation:

"To implement log-in and log-out procedures for user internet sessions, with passwords different to those for access to the normal fileserver."

This was on the basis that: *"No separate password controls are used for internet browser sessions and thus, there is a higher potential for colleagues to access web content (including unsuitable material) from an unattended machine. This also makes the disciplinary process harder to enforce if there is any doubt over the guilty party."*

However, at the time, this recommendation was not accepted as the officer responding indicated that the Authority had a single sign-on policy ie. once the user has logged-in, they are able to use their applications/services according to that account's rights throughout the day. It was agreed that a review of this policy would be conducted by April 2007.

It was not clear at the time, when the original recommendation was rejected, that a large number of generic accounts would operate, giving little/no opportunity to trace activity to specific individuals and thus inhibit any investigation / necessary disciplinary action.

With regard to internet sessions, it was felt by the Authority that the difficulty resided with the effort and time delays in users having to log-out (on shared machines) in order for others to log back in. In reality, staff would be unlikely to do this and thus, users could continue to use sessions initiated by their colleagues (and still potentially indicating it is them using the system).

Sandwell MBC operates an 'explicit authentication' for each internet session, via its proxy software. Basically, when a browser (eg. Internet Explorer) first attempts to connect to the internet, a pop-up box requires them to enter their ID and Password. After the browser is closed, re-starting it for a subsequent session again requires re-authentication. This process takes just a few seconds and fully supports the swift re-use by colleagues when necessary. It is possible that a similar facility can be incorporated within WMFS with little expenditure.

There was also a debate over users leaving their machines logged-in whilst away from their desk, and the opportunity for misuse to be attributed to the wrong person. The Authority at the time felt that this was not a problem. However, machines have been observed unattended on WMFS premises whilst still logged-in.

Furthermore, the authority has not implemented a time-out facility, after a period of inactivity. This could help minimise (though not resolve) the potential for unauthorised access via these unattended machines by colleagues.

Several existing systems (eg. the SMBC hosted Financials) currently require separate user authentication (therefore a complete single sign-on is not a reality). However, should the system be replaced and single sign-on implemented, there could be concerns over access controls and system security, under the existing account controls.

Recommendation 4

All Generic Accounts should be migrated to specifically named accounts.

Recommendation 5

A review of the general single sign-on policy should be undertaken, outlining both benefits and potential weaknesses. This should cover access to the internet and other sensitive/confidential systems eg. HR, Finance etc., audit / management control requirements, consideration of implementing re-authentication and options for resolving any identified issues.

4.11 Test 4 Adult Sites

We examined the logs for adult-related access attempts and if potential misuse was found, examined the preceding entries to determine the context to see if this was obviously deliberate access, or, merely accidental. This is intended to establish if it was clearly deliberate action to access this type of material, or, if these were triggered from innocent sites without user control (eg. pop-up banner ads).

There were only 904 lines of log entries related to this material (categories 65: Nudity, 66: Adult Content, 67: Sex), all such access successfully blocked by Websense. Looking at these, many appear to be Facebook photos which may/may not be correctly categorised. A number also appear to be Google images, again, these have not been tested.

Whilst these were indeed apparently (blocked) pornographic sites, they appear to have resulted from searches made for “sexy wallpapers” and a particular female model, such searches are likely to generate automatic pop-up links to other sites when clicking on an image.

Recommendations 6 and 7 elsewhere in this report address these issues.

4.12 Test 5 Internet Searches

We examined the search terms entered into Google, the most popular search site, to see if there was evidence of attempted misuse.

To preserve confidentiality of the officers concerned, the identities relating to the log entries was not included.

This was undertaken in order to ascertain whether anyone was deliberately searching for unsuitable material, and could give a clearer indication of this intent, rather than merely a log of a blocked site access which may result from accidental / pop-up activity.

108,637 lines were identified containing Google's common search string "search?hl", which precedes the text of the specific search terms. A visual scan of these was conducted and there were none found to contain anything of a pornographic nature.

As stated above, a small number were for "sexy wallpaper" whose results are likely to be automatically blocked anyway. It is not clear whether these resulted in any images being installed as 'wallpaper' on the users' machine, or, if it was merely for viewing the images.

4,241 log entries were for 'wallpaper' spread across 163 separate users and it is understood that users are allowed to select their own desktop wallpaper image, rather than there being a standard corporate image.

Recommendation 6

Consideration should be given to the standardisation of a corporate desktop wallpaper image.

Recommendation 7

If user-selected wallpapers are to be permitted, standards that should be met (ie. with regard to glamour/nudity, profanity, political etc.) should be clarified.

4.13 Test 6 Out of Hours use

We also attempted to examine Out of Hours access, as the risk of misuse is potentially greater at this time:

- Evening/Night staff - Possibly with less monitoring, and generic (non-traceable) accounts,
- Day staff - Whether staff are working longer periods, coming in or leaving at unusual times in order to misuse the service
- All staff - Whether their account log-on details have been compromised and the service is being used at times by other members of staff when the main account holder is not present. This can indicate passwords have been shared or, possibly discovered without their knowledge.

An extract was produced of all log entries before 8am or after 7pm however this was over two million records, relating to 1,739 separate accounts. It was therefore not possible at this stage to identify whether such usage is unusual without a fuller examination and knowledge of the working patterns of the individuals. The report can be provided to WMFS for examination if required.

Recommendation 8

Consideration should be given to The Out of Hours report produced during this audit being examined to check if internet usage is within expect / contracted periods for the named officers.

4.14 Test 7 Missing Users

We attempted to identify if there were any log entries for user accounts that were not present in the main Users file, as this could indicate hidden accounts to avoid normal analysis, potential administration problems or, simply, recently deleted accounts with prior usage.

No such records were found.

4.15 Test 8 Sample Alerts

Websense maintains various Threshold levels for the different categories. This allows emails to be triggered to inform an administrator of potential misuse when the threshold has been reached during one day.

At our visit on 28 November 2008, we were provided with copies of three recent alert emails (one adult, one malicious site, one spyware) in order to confirm that alerts were accurately identifying the user and that threshold levels were being calculated correctly.

Alert 1	Category 66 : Adult Content			Threshold: 20	
Date	25/11/08	Time	08:29:21	User	386
Findings	No log entries found for this user on that date. Further investigation revealed the omission of log entries for 28/10/08 to 26/11/08.				

Alert 2	Category 128 Malicious Sites			Threshold: 5	
Date	27/11/08	Time	13:59:53	User	662
Findings	Correct.				

Alert 3	Category 154 Spyware			Threshold: 5	
Date	27/11/08	Time	17:12:25	User	2795
Findings	Incorrect time, 5 th matching entry was 17:11:35, not 17:12:25				

Due to the omission of some of the relevant log data (period 28 October to 26 November), and the apparent time inaccuracy, it was not possible to confirm that alerts were correctly being generated, with accurate log entries to support the claim.

4.16 Test 9 Threshold Levels

We examined the thresholds to see if these were set at correct levels, as misuse may go unnoticed this is set too high. Similarly, low thresholds may result in too many alert emails. We were informed that the current threshold levels are the default values set by the software upon installation. There was no documentation to show any discussion or consideration of these levels.

Recommendation 9

A review should be conducted to ensure Threshold levels are set to appropriate values and, where generated, Alerts are fully & accurately evidenced by the log entries.

4.17 Test 10 Facebook

We examined the levels of use of the popular social networking site Facebook, as sites such as this have grown massively in popularity in recent years and may be seen as a convenient way to 'chat' to friends without using traditional email systems. As such, it is tempting to use these sites throughout the day, maintaining conversations in parallel to (or instead of) main work tasks. Following high levels recorded against generic user accounts, an examination was conducted for all accounts, with similar usage identified.

Recommendation 10

The Authority should decide upon whether sites such as Facebook will be permitted (ie. not blocked), what conditions of use should be adhered to (ie. not during working time) and to ensure that all staff are aware of this policy.

Recommendation 11

Consideration should be given as to whether an internal retrospective analysis of the log details examined during this audit (relating to Facebook access) will be required.

4.18 Test 11**Former Chief Fire Office Internet Logs**

Finally, we examined the internet logs of the former Chief Fire Officer in order to determine if there was any apparent evidence of misuse. We found no log entries that would suggest any misuse, whether in sites accessed/blocked or in any search terms

The priority of the findings and recommendations are categorised as follows:

Fundamental - action is imperative to ensure that internal control failure is rectified immediately.

Significant - action is required to prevent significant Breakdown of internal controls.

Merits attention - action is required to enhance the existing internal controls.

5 Action Plan

Para	Recommendation	Categorisation	Accepted Y/N	Management comment	Implementation date	Manager Responsible
1	<p>The Authority should agree the scope, period and responsibility for a regular analysis of the internet logs. We would recommend that this be at least monthly and include:</p> <ul style="list-style-type: none"> a) attempted access to adult material b) access to social networking sites (eg. Facebook) c) unexpected Out of Hours activity 	Significant	Y	<p>Analysis period to be Monthly.</p> <p>Logs to be created by ICT and analysed by Corporate Planning & Support.</p> <p>a) Attempted access to adult material included</p> <p>b) Access to all Social Networking sites to be blocked with the exception of You Tube which will be reported upon.</p> <p>c) Considered, but deemed to be impractical given the varying shift patterns in operation.</p> <p>Standing Order 1/20 states that '<i>Occasional and reasonable use of the Internet for personal purposes is regarded as acceptable</i>'.</p>	April 2009	<p>Creation = Strategic Head of ICT</p> <p>Analysis = Director Corporate Planning & support.</p>
2	All system generated Alerts should be promptly examined and appropriate action	Significant	Y	Logs to be created by ICT	April 2009	Creation =

The priority of the findings and recommendations are categorised as follows:

Fundamental - action is imperative to ensure that internal control failure is rectified immediately.

Significant - action is required to prevent significant Breakdown of internal controls.

Merits attention - action is required to enhance the existing internal controls.

5 Action Plan

Para	Recommendation	Categorisation	Accepted Y/N	Management comment	Implementation date	Manager Responsible
	taken and documented.			and analysed by Corporate Planning & Support.		Strategic Head of ICT Analysis = Director Corporate Planning & support.
3	The Websense Server Event logs should be examined on a daily basis and any corrective action taken as appropriate.	Merits attention	Y	New server in situ with an updated version of Websense loaded – There have been no failures to record logs since the upgrade. Log examination now built into ICT engineers' daily checks.	February 2009 Complete	Strategic Head of ICT
4	All Generic Accounts should be migrated to specifically named accounts.	Significant	Y	The following proposal will be issued for consultation: The current generic accounts will be addressed as follows: Group A: Internet Café type service. Allow 'white listed'	Consultation: March 2009 Implementation: April 2009.	Director Technical Services & Those responsible for Internet Café type service

The priority of the findings and recommendations are categorised as follows:

Fundamental - action is imperative to ensure that internal control failure is rectified immediately.

Significant - action is required to prevent significant Breakdown of internal controls.

Merits attention - action is required to enhance the existing internal controls.

5 Action Plan

Para	Recommendation	Categorisation	Accepted Y/N	Management comment	Implementation date	Manager Responsible
				<p>websites that are currently accessible with enforced implementation of logs as to who is using the PC (as per traditional internet café / library public access provision)</p> <p>Group B: Non-Internet Café: All internet access to be blocked for all other generic accounts.</p>		

Para	Recommendation	Categorisation	Accepted Y/N	Management comment	Implementation date	Manager Responsible
5	A review of the general single sign-on policy should be undertaken, outlining both benefits and potential weaknesses. This should cover access to the internet and other sensitive/confidential systems eg. HR, Finance etc., audit / management control requirements, consideration of implementing re-authentication and options for resolving any identified issued.	Significant	Y	<p>Having undertaken a review and considering the pro's and con's of Single Sign On (SSO), WMFS will maintain its SSO approach.</p> <p>As identified at point 3 of this report Websense appears to be working well.</p> <p>To further mitigate risk action will be to re-inform all staff that they are responsible for their logins and for any action taken against their login.</p> <p>To support this process a Routine Notice will be issued and Standing Orders updated to advise all staff of a) their responsibility and consequences for non-compliance b) that they are to use ctrl-alt-del keys to lock their computer when leaving their workstation c) an auto time out will be implemented, although this provides additional protection it does not negate the responsibility of the user to lock the device with ctrl-alt-del keys d) that there</p>	<p>Review February 2009.</p> <p>Issuing of instructions: May 2009</p> <p>May 2009</p>	<p>Director Corporate Planning & Support and Director Technical Services.</p>

Para	Recommendation	Categorisation	Accepted Y/N	Management comment	Implementation date	Manager Responsible
				has been a wording change at PC boot up to advise of 'acceptable use' (as per Standing Order 1/20) e) that the new monitoring process is to commence f) that enforcement of this area is to take place and g) that wallpaper and screensaver images must not be of a <i>harassing, defamatory, copyrighted or pornographic</i> nature. Standing Order 1/20 will be updated to include these instructions.		
6	Consideration should be given to the standardisation of a corporate desktop wallpaper image.	Merits attention	Y	After consideration of this matter it has been decided that WMFS will continue to allow individuals the ability to load their own wallpaper.	February 2009 Complete	Director Corporate Planning & support and Director Technical Services.
7	If user-selected wallpapers are to be permitted, standards that should be met (ie. with regard to glamour/nudity, profanity, political etc.) should be clarified.	Merits attention	Y	Staff to be reminded via Routine Notice and amended Standing Orders of the need to abide by WMFS' logon banner (which is accepted by clicking the 'OK' button each time a user logons on) and Standing	May 2009	Routine Notice & Standing Order amendments to be issued by Director

Para	Recommendation	Categorisation	Accepted Y/N	Management comment	Implementation date	Manager Responsible
				Order 01/20 with regards to the restrictions of use relating to images of a <i>harassing, defamatory, copyrighted or pornographic</i> nature (including politics and glamour).		Corporate Planning & Support and Director Technical Services.
8	Consideration should be given to the Out of Hours report produced during this audit being examined to check if internet usage is within expect / contracted periods for the named officers.	Merits attention	Y	<p>After consideration of the new monitoring processes being implemented and the pending issuing of the Routine Notice and Standing Order amendments referred to throughout this document, it has been decided that a retrospective approach is not to be adopted.</p> <p>As per number 1 above this specific area was deemed to be impractical given the varying shift patterns in operation.</p>	May 2009 Complete	Director Corporate Planning & support and Director Technical Services.
9	A review should be conducted to ensure threshold levels are set to appropriate values and, where generated, Alerts are fully & accurately evidenced by the log entries.	Significant	Y	A review is to take place of the logs and alerts identified in numbers 1 and 2 above.	April 2009	Strategic Head of ICT & Director Corporate Planning & support

Para	Recommendation	Categorisation	Accepted Y/N	Management comment	Implementation date	Manager Responsible
10	The Authority should decide upon whether sites such as Facebook will be permitted (ie. Not blocked), what conditions of use should be adhered to (ie. Not during working time) and to ensure that all staff are aware of this policy.	Significant	Y	Access to all Social Networking sites to be blocked. Access to You Tube will remain and it will be reported upon. (As per point 1 above)	April 2009	Creation = Strategic Head of ICT Analysis = Director Corporate Planning & support.
11	Consideration should be given as to whether an internal retrospective analysis of the log details examined during this audit (relating to Facebook access) will be required.	Merits attention	Y	After consideration of the new monitoring processes being implemented and the issuing of the Routine Notice and Standing Order amendments referred to throughout this document, it has been decided that a retrospective approach is not to be adopted. (As per number 8 above.)	May 2009 Complete	Director Corporate Planning & support and Director Technical Services.