Employee ICT Health Check

KJB Computer Forensics

Jim Borwick MSc

Introduction

Increasingly companies are becoming more reliant on the internet for business use; however with this comes the problem of employee abuse of the internet. In the past employees used to waste time in break rooms drinking coffee now they are wasting time on the internet for non business use, cyber-slacking.

The aim of this document is to highlight the extent of the abuse of company internet connections and what we can do to assist you to deal with it appropriately.

It stands to reason that Cyber –Slacking is not acceptable, employers should be aware of the issues associated with unauthorised internet use, some of which include:

- Loss of productivity - Employees conducting personal business during company time.
- Legal Issues - Employees downloading copyrighted software or facilitating the sharing of copyrighted material via file sharing websites.
- Employee Harassment – (Sexual, Racial, Social etc) Viewing explicit material on company time and company computers.
- Bandwidth issues - Non business internet use can slow your company network server.
- Earning another income on company Time - Some websites offer cash to surfers and e-mail readers.
- Infection of company servers/networks - The risk of infecting the company network with viruses and malware[1] increases if employees are accessing unauthorised websites. This can be very costly in time and more importantly can open the company network to a selection of security threats, which raises issues with the company's ability to secure data.
- Theft of Intellectual Property – The longer unauthorised internet use is left unchecked the greater the risk of a breach of client confidentiality or worse still theft of client information.

[1] Malware, short for *malicious software*, is software designed to infiltrate a computer system without the owner's informed consent. Software is considered to be malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, crimeware, most rootkits, and other malicious and unwanted software.

KJB Computer Forensics
15 High Street,
Dunbar
Tel: 07748736481
Email:jim@kjcomputerforensics.com
Website: www.kjcomputerforensics.com

Scary Statistics

Employee Computer & Internet Abuse Statistics

In a recent online survey the following statistics were discovered:

- 30 to 40% of Internet use in the workplace is not related to business.
- 64% of employees say they use the Internet for personal interest during working hours
- 70% of all Internet porn traffic occurs during the nine-to-five work day.
- 37% of workers say they surf the Web constantly at work.
- According to a survey by International Data Corp (IDC), 30 to 40% of internet access is spent on non work related browsing, and a staggering 60% of all online purchases are made during working hours.
- 90 percent of employees feel the Internet can be addictive, and 41 percent admit to personal surfing at work for more than three hours per week.
- Around 80% of computer crime is committed by "insiders". They manage to steal £100 million by some estimates; £1 billion by others.
- 25% of corporate Internet traffic is considered to be "unrelated to work".
- 30-40% of lost productivity is accounted for by cyber-slacking.
- Most studies show 70% of companies have had sex sites accessed using their network.
- When asked "should employers monitor, limit, block or control your Internet access while at work?" over 60 % of employees said "yes".
- Traditionally, employers have been responsible and liable for the actions of their employees in the workplace. However, if an organisation can demonstrate a "duty of care" to reduce unacceptable employee activity, then it could minimize its potential for liability.
- A company with 1,000 Internet users could lose upwards of £35 million in productivity annually from just an hour of daily Web surfing by employees
- It is estimated that the greatest threat to intellectual property is trusted insiders; 70% of security breaches come from inside.

What can you do?

There is the potential for some very serious repercussions if you allow unlimited, unmonitored usage of the internet by your employees during work hours. Whilst it may not be practical to prevent all access to the internet you should at the very least consider implementing an employee internet usage policy. If you do not have such a policy in place we can advise accordingly.

KJB Computer Forensics
15 High Street,
Dunbar
Tel: 07748736481
Email:jim@kjcomputerforensics.com
Website: www.kjcomputerforensics.com

What can KJB Computer Forensics do for you?

Having an internet usage policy can reduce the risk of the abuse of the internet but will never eliminate the risk completely. In cases where you suspect an employee is abusing the company's internet access you need to be able to deal with it in a professional manner.

It is important that when gathering computer based evidence in relation to an abuse of company policy, that it is done in a forensically sound manner. The following points should be noted when dealing with electronic evidence:

- No action should be taken that will change data held on a computer which may be subsequently used in a tribunal or other disciplinary hearing.
- Where it is deemed necessary to access original data held on a computer, that person must be competent to do so and be able to explain the relevance and the implications of their actions.
- An audit trail recording all actions/processes applied to computer based electronic evidence should be created and preserved.

These points should be adhered to as they protect the rights of the employee and just as important the rights of you the employer. Here at KJB Computer Forensics we are competent and very experienced in working within the aforementioned guidelines.

Employee ICT Health-check

One of the many services that KJB Computer Forensics offers is an Employee ICT Health-Check.

The ICT Health-Check would take the form of inserting a USB device into a particular computer and recovering data files which will show exactly what your employee has been doing on their computer and when.

KJB Computer Forensics
15 High Street,
Dunbar
Tel: 07748736481
Email:jim@kjcomputerforensics.com
Website: www.kjcomputerforensics.com

Examples of the type of information that we can recover are as follows:

- Internet History
    - Internet history will reveals the times, dates, websites visited, number of times a particular website is visited and the name of the person logged in at the time.
    - Internet History will also reveal a user's activity on social networking websites such as Facebook, Bebo, Second Life etc.
    - References to web based email such as Hotmail or Gmail. Both of these web based email providers also offer online storage. This could facilitate the theft of client or company information by merely uploading the data to the online storage. There would be no need for the 'rogue' employee to try and smuggle data of the premises on USB stick, merely upload using your resources.
    - References to online storage such as Dropbox or BT's Digital Vault. These present the same risks as outlined above.
    - References to file sharing websites. Apart from the obvious dangers of employees using your resources to share copyrighted software, these sites are also rife with viruses and malware – a huge security risk to your company network.
- Internet Search History
    - What search terms have been entered – search terms specifically entered by the computer user.
    - References to the particular search engine used to perform the search.
- Access to Sexually Explicit material
    - Our ICT Health-Check can quickly identify if an employee has accessed illicit material online e.g. pornography etc. You may think this is preposterous, the above statistics tell a different story.
- Instant messaging
    - Instant messenger software such as MSN messenger etc is another threat to the security of confidential information.
    - It is possible to transfer files via messaging software.
    - It is possible to recover chat logs showing conversations.
- Access to FTP sites
    - An FTP site is similar to a website only not as searchable i.e. you need to know its web address to access it, making FTP sites almost invisible.

KJB Computer Forensics
15 High Street,
Dunbar
Tel: 07748736481
Email:jim@kjcomputerforensics.com
Website: www.kjcomputerforensics.com

    - File Transfer Protocol (FTP) allows the computer user to upload/download files to an online storage area. This function is almost always overlooked by IT staff when setting up security restrictions.
    - An example of a potential use of this would be to upload files directly from a company network to a FTP website. These files can then be accessed from anywhere in the world provided there is an internet connection. The dangers here are obvious – theft of intellectual property or confidential client information.
- File Sharing
    - File Sharing can be facilitated through software such as Limewire, Bittorrent and even web based email hotmail.
    - This is another serious danger to a company network which at its best reduces the bandwidth of the company network, at worst facilitates the illegal sharing of copyrighted software material.
- File Access
    - It is possible to show what files/documents have been accessed.
    - This is of particular interest as it may highlight unauthorised access to confidential information or files which that particular employee should not be accessing.
- Recycle Bin
    - The recycle bin can contain invaluable information.
    - The recycle bin can show references to information which the computer user may be trying to hide.
- Wireless connectivity
    - Where the company uses wireless enabled laptops there is then the danger that this facility may be abused e.g. Is it connected to a wireless router other than your company router during working hours?
    - Is the employee then using this 'other' connection to facilitate file sharing or transfer of confidential information?
- Use of USB devices.
    - This is a real security risk and relatively easy to resolve but very rarely addressed by company IT teams.
    - We can show how many USB devices have been inserted into a particular computer.
    - It is sometimes possible to show when files have been transferred to USB devices.

KJB Computer Forensics
15 High Street,
Dunbar
Tel: 07748736481
Email:jim@kjcomputerforensics.com
Website: www.kjcomputerforensics.com

This list is by no means exhaustive; these are merely examples of information which we can recover. Our ICT Health-check can be tailored to suit your particular needs. Call for more information or to arrange a meeting to discuss further.

Employee ICT Health-Check Report

We will produce a user-friendly report together with all information gathered at the time of the examination. The report will give you a detailed explanation of all facts gleaned during the investigation and recommendations we consider relevant. Our report will be to a standard acceptable for use at any tribunal or disciplinary hearing, which we will attend in person if required.

Our Expertise

The Managing Director (MD) served in HM Forces for 24 years, serving with the Royal Military Police and the 1Bn Queens Own Highlanders. Following a successful military career the MD moved on to serve within law enforcement in Scotland. The MD has a Masters Degree in Computer Forensics and a wealth of experience with criminal investigations within the Scottish judicial system.

KJB Computer Forensics' examiners are experts at securing digital evidence and the investigation of all manners of digital crime. We are educated to degree level, have worked within law enforcement and are security vetted to SC level. Our evidence is produced to a standard acceptable within Scottish and English Courts. We have given oral evidence in the High Court on numerous occasions.

KJB Computer Forensics
15 High Street,
Dunbar
Tel: 07748736481
Email:jim@kjcomputerforensics.com
Website: www.kjcomputerforensics.com

Summary

In today's modern culture we are all used to being afforded a far greater freedom of use of the internet at home and during the working day. However, it is important that your employees are aware of the extent of this freedom with regards to the use of company internet access. It is also important that you the employer have appropriate policies in place which provide the employee with clear guidance as to the use of the internet whilst at work.

Where an employee fails to adhere to the company internet usage policy, the individual(s) must be dealt with appropriately and fairly.

Failure to take action where abuse of your internet connection has occurred will increase the risk of loss of confidential information, risk the integrity of your company and its network and ultimately increase the risk of great financial loss to you or your company.

Ultimately you are responsible for the electronic well being of your employees and company assets.

Jim Borwick MSc
Managing Director KJB Computer Forensics
Tel: 07748736481
Email: jim@kjbcomputerforensics.com
Website: www.kjbcomputerforensics.com