

Release date: 3rd October 2007

**Computer Evidence in Employment Tribunals;
'What are your staff up to from nine to five?'**

More offices are moving towards being paperless, with staff having full access to internal and external emails, the internet, and, networked company files.

However with workstations shielded by partitions, backs to the wall and slack IT usage policies, the lure of working for competitors, circulating office gossip, and surfing online can prove too tempting for some employees. With millions of working hours being lost each year through email and Internet misuse, and intellectual property theft a serious concern for employers, exactly what staff up to from nine to five?

Internet and Emails

Lengthy periods spent on Facebook, EBay, and Christmas Shopping online costs employers millions in lost working hours every year. To monitor this, companies should have in place Acceptable Use Policies (AUP's) as regards the absolute perimeters of using the Internet and emails in the workplace.

Seems simple enough, however, many companies are still very blasé about their IT security, even though major breaches can have significant consequences. Employment tribunals and court cases can actually leave the employer vulnerable to allegations of constructive and wrongful dismissal. Major breaches could include accessing pornographic or illegal websites, or substantial claims of harassment, discrimination or bullying in the workplace.

Pro actively responding to an AUP breach is crucial in terms of damage limitation and

MORE

securing evidence to discipline an employee. More often than not, the guilty employee will have tried to disguise their activities; deleting their Internet history and any offending emails. This makes the situation harder to prove and involves the recovery of data which is normally beyond the remit of the average IT team. There is also the issue of objectivity to consider if the case is likely to go to tribunal or court proceedings. It is at this stage that most IT savvy directors will call in a third party computer forensics team.

By employing experts in the trade, all evidence will actually be recovered not only objectively, but in compliance with the Association of Chief Police Officer guidelines, with a clear audit trail and signed witness statements. Full Internet history logs can be recovered detailing the websites visited, time spent on each site, contents of emails, dates and so on. The evidence is recovered, secured, and can be used to confront the employee or retained to build up a stronger case against an individual.

Theft of intellectual property

Intellectual property is one of a business's most important assets but is often left unprotected and accessible to the dishonest employee. Business development plans, customer databases, product specifications, accounts information can be invaluable commodities if, for example, an employee is poached by a competitor.

The dishonest employee is becoming more adept at carrying out such offences. Most are now quite sophisticated and will go beyond simply emailing information from the workplace to a private email address. Mobile phones, iPods and thumb drives can be used to download and save information to discreetly, in a lunch hour perhaps or when working late. These tracks can be covered quite simply though, and it is only through forensic analysis of the computer hard drive that the criminals movements can be identified and report on.

MORE

Another favourite pastime of the aggrieved employee is to password protect or change the password of key documents /databases before they leave. Skilled forensic investigators can crack passwords relatively simply using hi tech software not guesswork, and business as normal can resume fair quickly. They can also show through analysis which employee had access to what and when. These reports can prove critical in the prosecution of a case; they are independent, objective and non disputable.

Carrie Moss

Marketing Executive CY4OR

info@cy4or.co.uk
www.CY4OR.co.uk
0161 797 8123

ENDS...

Contact Carrie Moss
0161 797 8123
Carrie.moss@cy4or.co.uk

NOTE TO EDITORS

If you would like to sample any part of this release do please let Carrie or any member of the CY4OR team know. CY4OR is a Law Society registered firm and approved Expert Witnesses. Our core service offering includes Computer Forensics, Mobile Phone Analysis, E Discovery, Document Analysis and Forensic Audio & Visual Enhancement.