

EMPLOYEES – ASSET OR RISK?

There has been an 81% increase in the cost of employee fraud over the past two years. A factor could be that fidelity is no longer key to today's increasingly mobile workforces and technology, and user competence is gathering pace at an astonishing speed. This creates a challenge for organisations in terms of their desk-top/digital security procedures, so forcing them to look closely at the mechanisms they use to combat computer misuse issues in the future.

Is it worth it?

Recent findings suggest the cost of computer enabled financial fraud in 2004 was £622 million, with an average of 35 incidents of financial fraud per organisation. Scratch under the surface, however, and you will find that stolen intellectual property and criminal court cases against employers could hide a much greater cost.

Digital forensics has historically been a reactive response to the problem. However, many organisations are now becoming proactive in their fight against employee digital crime and misuse.

How much time do your employees spend on personal internet/email?

The most common reason for disciplinary action in the UK is the sending of unauthorised emails. Studies show that 27% of Fortune 500 companies have fought email harassment claims, yet most do not realise the consequences of email and internet misuse. Renfrewshire Council learned the hard way and was recently in the headlines after dismissing nine employees for inappropriate use of email.

By instructing a digital forensics expert you are ensuring the collection of digital evidence in a forensically scientific manner. Unlike internal IT departments, forensic experts are dedicated purely to digital forensics and conduct all investigations following Association of Chief Police Officers guidelines for the collection and preservation of digital evidence; and, of course, their impartiality can never be questioned by a court or tribunal.

Organisations are starting to realise their employees are not only their greatest asset, but also their largest risk.

Sophie Gilkes and Clare Brett report



Using specialist forensic software the analyst can access information, such as last internet site visited and user and internet history. Investigations can focus on a specific period of time, running key words to identify documents pertaining to the client's objectives.

Nearly two-thirds of organisations are taking action against the misuse of email and internet by restricting the use of private email accounts and internet usage, including banning certain sites. The number of email and internet misuse cases reaching tribunals is ever increasing and digital forensics companies see the need for organisations to understand the importance of preserving evidence, just as a police officer would at a murder scene.

Intellectual property theft has never been easier

Intellectual property is the backbone of an organisation. Many companies risk losing sensitive data because of a failure to secure or restrict electronic devices used by their employees. Currently, 40% of organisations do not apply the same security processes to digital devices as they do to a laptop, yet a PDA can now contain just as much relevant information!

So what can be done if an organisation suspects an employee of stealing intellectual property? A forensic analyst can examine the suspect's computer to determine if the information has been downloaded to removable media (CD, DVD, USB sticks etc) and determine times when this occurred. This information can then be used to commence proceedings.

Organisations can fight back

Proactively, organisations can put in place a clear, concise AUP policy and communicate this to all employees. Partnering with a digital forensics company and stating as much, gives the message that misuse is taken seriously. Employees then know that their actions will be monitored and action taken should computer misuse be detected.



Reactively, even if an incident has occurred, organisations can still minimise their exposure by following the guidelines below. A digital forensics organisation will work with the client to implement a plan to recover the maximum amount of evidentiary material.

You are not alone!

To minimise business disruption, a digital forensics company can complete the process of imaging (copying) hard drives outside of working hours, returning with the image to their laboratory where they will conduct their analysis. Some may provide written "Guidelines in Cases of Suspected Computer Misuse" and most will offer a 24/7 helpline for advice when an incident is first discovered, and in urgent cases can attend to secure evidence at a few hours notice.

Nearly two-thirds of organisations are taking action against the misuse of email and internet by restricting the use of private email accounts and internet usage, including banning certain sites.

Typical guidelines in cases of suspected computer misuse would be:

- Treat it seriously.
- Keep it to yourself.
- Do not alert the suspect to the investigation.
- Do not involve your IT department.
- If the computer is off – do not switch on.
- If the computer is on – document what is on the screen and pull the plug from the wall.
- Make notes of everything you do.
- Call in the experts or at least call them to get advice!

Sophie Gilkes and Clare Brett are with CCL-Forensics Ltd
01789 261 200
www.ccl-forensics.com