

**Release date: 11<sup>th</sup> January 2005**

**Are you sitting next to a criminal?**

Computer criminals could be working next to you every day, yet be stealing from your business.

A survey carried out on 201 companies by the National High Tech Crime Unit, found that the impact of hi-tech crime in 2003 reached an estimated £195 million. Acts of data theft and sabotage were usually found to be internally originated. More worryingly, over one third of fraud acts involved company employees.

There are various reasons that these crimes can occur; usually crimes are carried out by disgruntled employees who feel the company has treated them unfairly. Employees lower down in the hierarchy may take advantage of loopholes that they see in the system. Data theft can often occur by employees leaving to set up a rival company or data is stolen to sell on to rival companies. People carrying out computer crime may distance themselves from the reality that they are breaking the law as it is depersonalised by computers, however the crime can be just as serious and devastating as mugging somebody on the street. Computer crime is simply old crimes committed using new tools. If the perpetrators aren't caught, companies are at a huge financial risk, not to mention the risk to company image and reputation once a breach occurs.

There are now plenty of companies who can provide security solutions that go some way to protecting company information stored on computers. However, companies also need to be aware of the steps they need to take if the unthinkable happens. Major problems can arise if companies try and sweep the problem under the carpet or let the perpetrator get away with the crime. Often companies are worried about the cost of using experts to document the crime, however the costs of ignoring the problem can be far greater.

**MORE**

Computer Forensics companies can help once a security breach has occurred. Computer forensics companies specialise in gathering evidence from computer media. This Information can then be used in a court of law if necessary as evidential continuity is upheld.

Companies are often worried about carrying out an investigation and the possible disruption to business continuity. In addition they may be worried that employees will find out that a breach has occurred, especially if the suspect is still working for the company. A Computer Forensics company should be used to carrying out covert operations, often outside working hours in a discrete and timely fashion, causing minimum disruption.

If a breach has occurred in an organisation the temptation for that organisation is to either have a look at the computer themselves or hand it over to their IT department. The damage that these actions have is that those people do not know what they are looking for and in the fifteen minutes that they look around they will change the data, meaning that if the data is required as evidence it may not be valid.

You wouldn't ask your sales team to look after your accounts system or employee contracts so why ask your IT department to look after your computer forensics. A specialist computer forensics company should have had specific training and will know to obey the ACPO (Association of Chief Police Officers) guidelines. A computer forensics expert should know exactly where to look for information without compromising evidential continuity.

### **When a security breach occurs, what steps should an organisation take?**

- **Do treat the matter of computer crime seriously.** The people that commit this crime depersonalise it, as humans do not appear to be involved, however the damages can have severe affects on your business as well as your health and well being.

MORE

- **Do not tell anyone about your suspicions** unless they really need to know as rumours do spread like wildfire.
- **Do not challenge the target with your concerns.** If they are up to no good you're simply going to alert them that you're on to them.
- **Do not let your own IT department have a quick look** at the computer media as this can damage the evidence and yield it useless in a court of law. You would not ask a conveyance solicitor to look at a murder trial, therefore an IT person should not look at the computer as computer forensics have had specialist training. A computer forensic will obey ACPO (Association of Chief Police Officers) guidelines to ensure evidential continuity is upheld and that certain standards are complied with.
- **Do take legal advice before beginning a covert investigation.** We live in a very litigious society and you could end up on the wrong side of a court case for all the wrong reasons.
- **Do not switch the computer on** if possible as every time a computer is switched on data can be changed. Computer forensic analysts use special forensic tools to ensure that when they investigate the computer no changes are made to the digital evidence.
- **Do make notes** as to who has used the computer and any other information you may have, however remember that they may have to be surrendered to the other side at some point if the case progresses to court.

CY4OR provides a number of proactive and reactive computer forensic investigation services to the public and private sector including law enforcement agencies, solicitors and corporate companies.

**[info@cy4or.co.uk](mailto:info@cy4or.co.uk)**  
**[www.CY4OR.co.uk](http://www.CY4OR.co.uk)**  
**0161 797 8123**

**ENDS...**

**Contact Carrie Moss**  
**0161 797 8123**  
**[Carrie.moss@cy4or.co.uk](mailto: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.

Copyright CY4OR