

REVEALING FACTS, PRESENTING EVIDENCE

By Sally Ramage®



The Computer and Internet Crime Conference 2004 which took place in London on the 30th and 31st March was a very necessary and timely conference . Ed Gibson, Agent of the FBI and now at the US Embassy, gave a presentation , the opening address made by the Assistant Commissioner of the Metropolitan Police Tarique Ghaffer.

[\[1\]](#)

Cybercrime such as internal and external hacking , spam and computer viruses are widely acknowledged. Hacking is a growing problem for businesses which store confidential client and customer details electronically. External hackers can access confidential information, deface websites and steal financial company information.

Often, white collar crime is carried out by internal hackers but a larger proportion is through an outside source of security breaches. Employees can steal intellectual property from their employers. Intellectual property theft includes theft of e-mail address books, proposal documents used as marketing tools of solicitors, client databases and contact information. An indication on how serious the problem of white collar crime has become is the recent issue of “The Lawyer” which concentrated on the war on fraud and featured so many expert witnesses on white collar

crime.

In what way are hackers' activities illegal ? In the UK, it is a Data Protection Act offence to send unsolicited e-mails . There is a new European Commission Directive introduced in 2003 which makes it a criminal offence to send unsolicited e-mails. In the UK, this EC Directive has been implemented by the Privacy and Electronic Communications Regulations 2003. Will these regulations deter the sending of spam? Only if the source of the spam can be pin-pointed. Spam is

[2]
particularly sinister. At present spammers have created virtual countries' websites and virtual banks even. Spammers can blackmail companies. Current anti-spam devices can filter spam. Spam also damage businesses by taking up valuable business time in dealing with them and also because they can carry malicious viruses which cause even more major disruption to businesses . Viruses in a business's computer system are very costly in terms of data recovery, slow-down in productivity, necessary software upgrades as well as loss of business, not to mention the lowering

[3]
of staff morale and the damage to the business reputation . Internet filtering and e-mail monitoring software, anti-virus software , backing-up of data, and systems security policies are steps to controlling any potential damage. Staff policies must be put in place. The consequences of e-mail misuse must be set down in company policies.

If staff , for example, use e-mail to circulate ridicule about other staff members, this would amount to gross misconduct and dismissal. Such e-mails would amount to intrusions into employee privacy as per Article 8 of the European Convention on Human Rights.

When things go wrong, electronic documents, spread-sheets and e-mails hold the relevant material for litigation. More and more in court cases, evidence is found to be exclusively in electronic format. Forensic technology therefore needs to be a large part of the investigation. Forensic technology can recover, for example, deleted material. Forensic techniques can

recover multiple versions of the same document from traces left on electronic media. Small differences between the altered versions can be used to build up a picture of what changes were made and when. The time-line of document creation and differing versions can be used to corroborate or disprove the chronology of events. Electronic evidence must prove the provenance of the material and the entire history of electronic material can be collated to produce robust evidence in court. The evidence must be collected under the UK evidence laws. Metadata is hidden within electronic files, examples of which are entries in e-mails, dates embedded in documents and links to other files. In the case of e-mails, a full audit trail does exist and can be retrieved.

It is now possible for forensic technology specialists to use forensic tools to sift large volumes of material for electronic files and filter such material to reveal potential disclosable material. The volume of material in large businesses can be in terabytes in size. This material can be sifted on live computer servers without disrupting business or alerting any suspects.

And when a fraud case comes before the courts, evidence is displayed in court on large computer screens to the jury and the defence, rather than on paper. However, most successful prosecutions rely on more than one stream of computer-derived evidence. What is needed is more than one independent stream of evidence, oral, paper and computer-derived, which collaborate each other. There are cases where e-mails have been forged and it is no longer the case that because it is in electronic form, it must be true. A recent case in the UK is R v Bhatt (unreported) Canterbury Crown Court [2003]. During the trial, the defence illustrated to the court how such an e-mail is forged by simulating a link to the Internet to create and explain how electronic communications can be manipulated in real time. The simulated e-mail was “read” with a standard e-mail client, Microsoft Outlook Express and it appeared no different from the paper e-mails that the

prosecution offered as “proof” that the e-mail had in fact been sent by Bhatt. Only a full technical examination of the “headers” within Outlook Express system would have revealed the forgery, and only after a significant amount of network investigation.

So what can accounting departments do ? A fraud policy can be formulated. A fraud policy is a formal, written statement recording the company’s attitude to fraud. It should make clear that fraud is unacceptable and that all instances of suspected fraud will be treated seriously and dealt with swiftly. Staff should be required to indicate their awareness of and compliance with the fraud policy on an annual basis. The policy will serve a useful purpose as a deterrent. The company should also have a contingency plan setting out the steps that should be taken in the event that fraud is suspected. This plan should be known to all staff .

ENDS

[1]

Deloitte-Touche Tohmatsu 2003 Global Security Survey. 41% breaches carried out by outside sources, 24% of unknown sources and 35% by internal means.

[2]

The Assistant Commissioner of the Metropolitan Police said that recently a virtual country called “The Principality of Ceylon” was set up as a website.

[3]

The world’s most valuable brands are as follows:

Coco Cola \$70.45 billion, Microsoft \$65.17 billion, IBM \$51.77 billion, GE \$42.34 billion, Intel \$31.11 billion, Nokia \$29.44 billion, Disney \$28.04 billion, McDonald’s \$ 24.70 billion, Marlboro \$22.18 billion, Mercedes \$21.37 billion.

Source: Interbrand 100 Best Global Brands 2003.