

Fraud: Getting facts and presenting the evidence

Who are the bad guys in cyberspace?

Sally Ramage reports on the Computer and Internet Crime Conference 2004

The Computer and Internet Crime Conference 2004, which took place in London from 30-31 March, was a very necessary and timely event. It was also a high-profile one – Ed Gibson of the US Embassy gave a presentation, and the opening address was by Tarique Ghaffur (pictured), Assistant Commissioner in the Specialist Crime Directorate of the Metropolitan Police.

Other speakers and contributors included Eoghan Casey, a US specialist in the field and author of *Digital Evidence and Computer Crime*, Caroline Flint MP, a Home Office minister, Penny Harper of Bond Solon, Peter Wood from First Base Technologies (pictured) and Robert Jones of the University of London.

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

But often, white-collar crime is carried out by internal hackers. Employees can steal intellectual property from their employers – this might include theft of e-mail address books, proposal documents, client databases and contact information. An indication of how serious this problem has become was the publication of an issue of *The Lawyer* focused entirely on the 'war on fraud'.

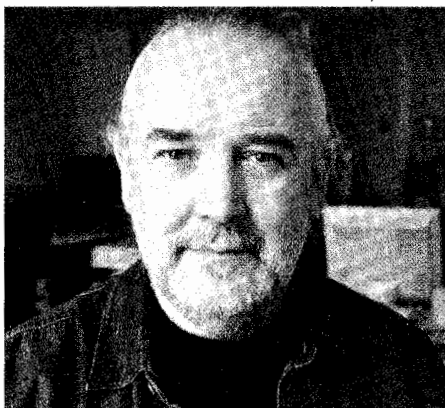
Another hot topic at the conference was spam. In the UK, it is a Data Protection Act offence to send unsolicited e-mails. An EC Directive introduced in 2003 (implemented in the UK by the Privacy & Electronic Communications Regulations 2003) also makes it a criminal offence to send unsolicited e-mails. Will these regulations deter the sending of spam? Only if the source of the spam can be pinpointed.

Spam is particularly sinister. Spammers have created virtual countries and virtual banks. Spammers can blackmail companies, and spam in any case takes up valuable business time and can carry malicious viruses that cause yet more disruption and damage to business' reputation.

An important message of the conference was



Ghaffur: The Met officer was a keynote speaker



Wood: One of several IT industry contributors

that the consequences of e-mail misuse must be set down in company policies. If, for example, staff use e-mail to ridicule other staff members, this would amount to gross misconduct. And such e-mails would amount to intrusions into employee privacy according to Article 8 of the European Convention on Human Rights.

When things go wrong, electronic documents hold the relevant material for litigation, and forensic technology therefore needs to be a large part of the investigation. Forensic technology can recover, for example, multiple versions of the same document and small differences between the altered versions can be used to build up a picture. The entire history of electronic material can be collated to produce robust evidence in court, as long as it is collected in compliance with UK evidence laws.

The coverage of this area by the conference

How big is this problem?

In research commissioned by the UK's **National High-Tech Crime Unit** in 2002, private-sector organisations were asked a number of questions about computer crime:

What did respondents consider the most serious impact of a computer-enabled crime?
 Ability to operate and function: 34%
 Ability to do business with customers: 32%
 Public image or reputation: 23%
 Finances of the company: 7%
 Share price of the company: 4%

How many had experienced such a crime?
 Virus attacks: 67%
 Financial fraud: 16%
 Theft of proprietary information: 15%
 Attacks (such as denial of service): 20%
 Theft of laptops: 77%
 Unauthorised website access/misuse: 18%
 Spoofing attacks: 13%
 Theft of other hardware: 40%
 Telecommunications fraud: 6%
 Telecoms eavesdropping: 6%

Percentage of total company spend given to prevention of such crimes:
 Less than one percent: 34%
 One percent: 12%
 Two-five percent: 22%
 Six to 10 percent: 6%
 Don't know/refused: 26%

was rich in new facts. It is now possible, for example, for forensic technology specialists 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, but 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 on large computer screens, rather than on paper.

What can accounting departments do about fraud? 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 asked to indicate their awareness of and compliance with the fraud policy on an annual basis. A 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.