The computer fraud conspiracy of silence

It can be tricky for companies to prosecute hackers. Lindsay Nicolle and Tony Collins report

WHEN a company discovers it has been defrauded by one of its own computer staff, the question of whether to prosecute is never easily answered.

First the company tries to determine how the fraud was perpetrated, to retrace the steps of the rogue computer programmer.

But some computer systems are so complex, extending to a network spanning several countries, that the task of pinpointing a single weakness which has been exploited by a knowledgeable insider is difficult, sometimes even economically unrealistic.

With some large-scale crimes, money is transferred by computer to different banks in various countries before ending up in a Swiss account.

Companies rarely call the police, believing that the resources available to detectives are insufficient to deal with a crime. Firms also suspect that computer law is too vague to support a prosecution.

Moreover, company directors fear that a police investigation may disrupt the day-to-day running of the computer department and, should news of an inquiry leak out, the confidence of investors in the company could be damaged. The shareholders may even demand the resignations of those responsible for the security of the systems.

Some firms are so anxious to prevent the police finding out about the crime that they sign legal "non-disclosure" agreements with the criminals, according to Rodney Hylton-Potts, a leading solicitor.

As part of such deals, the swindlers tell their employers how the fraud was carried out.

Mr Hylton-Potts said: "Many boards of directors consider that their duty is best discharged by not punishing the culprit."

In at least one agreement drawn up by Mr Hylton-Potts on behalf of a large financial institution, a person suspected of fraud was allowed to escape prosecution in return for paying back the money. Part of the contract said: "The employee has been accused by the employer of fraudulently obtaining a benefit in relation to a computer system within the ownership of the employer. The parties have agreed that no action will be taken to inform third parties of such allegations, including the police."

In this case the money paid back was £50,000, but there have been other occasions, said Mr Hylton-Potts, when the sums have been far higher — and much of it has been spent by the time the crime is detected.

Because of the secrecy surrounding such deals, the scale of computer crime cannot be known with any certainty.

One of the lowest estimates is from the Confederation of British Industry, which puts losses at £400m a year. UK consultancy PA says the figure could be £2.5bn.

Another consultancy, Touche Ross, is collecting evidence of computer hacking by setting up a confidential "hotline".

It reports that so far 50 companies, mostly from the financial sector, have rung the hotline giving details of hacking incidents.

Soon Touche Ross intends to pass the statistics on computer crime to Emma Nicholson MP in support of her efforts to make hacking a criminal offence.

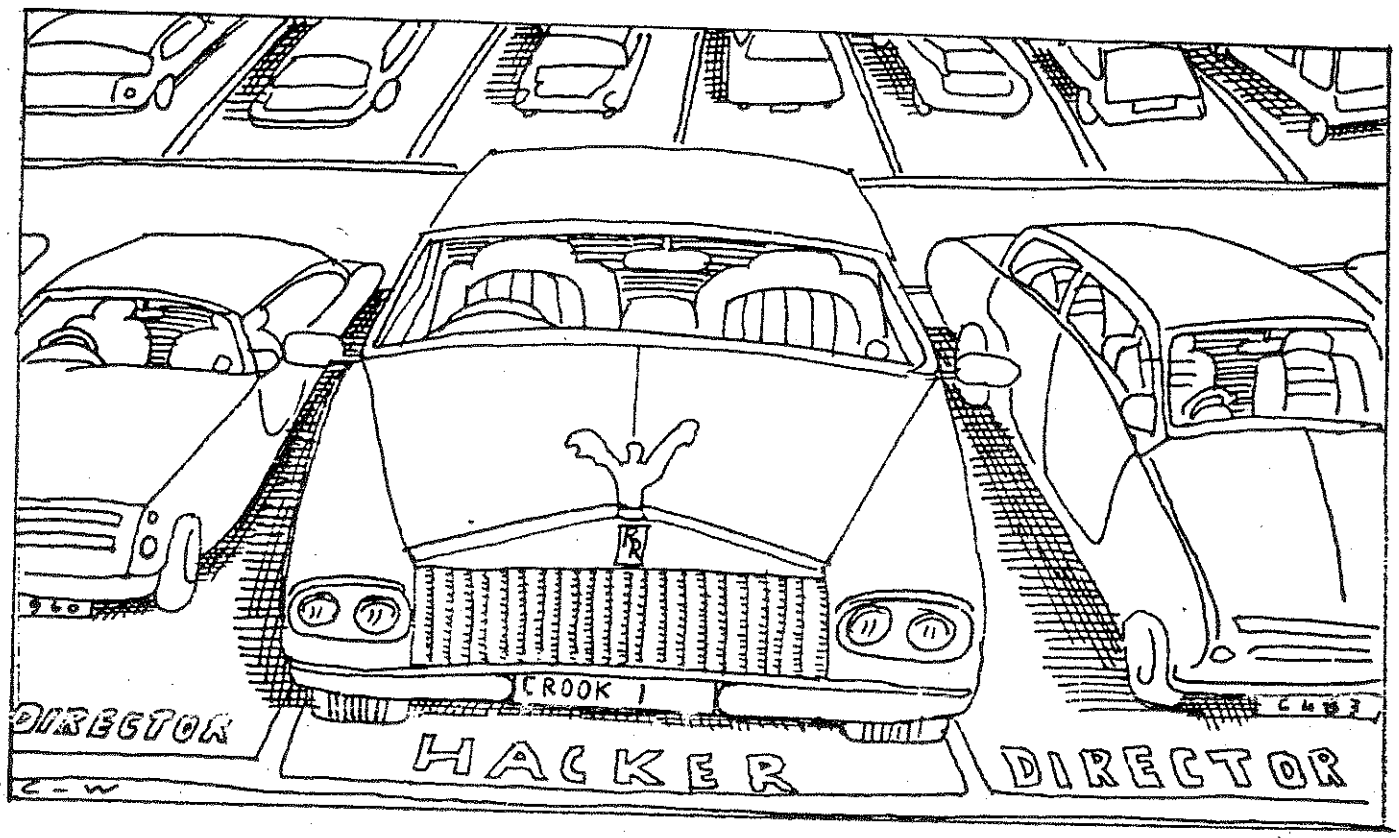
Ken Slater, a principal consultant with Touche Ross, said: "Reports are coming in quickly, after a slow start while organisations sought high-level permission to disclose their problems.

"Most of the cases are hackers on the inside of the organisations, employees who misuse passwords, browse in boredom, and corrupt chunks of database accidentally rather than deliberately."

He said some organisations had suffered losses of between £50,000 and £100,000. Much of this is the cost of recreating destroyed data. "In some cases it has taken six weeks to recreate transactions and restore each day's processing, which is quite a massive feat in terms of manpower."

Most of the companies ringing the hotline have not reported the in-

SCIENCE AND TECHNOLOGY is edited by **Tom Wilkie**



cidents to police. "They say they don't think the police would be able to cope with something as complex as this and they're terrified of adverse publicity," said Mr Slater.

The police disagree. "It's rubbish to say that we can't cope with hacking incidents," said Noel Bonozoszek, a detective constable in the computer crime unit of the Fraud Squad.

"We can call on any experts we need, as in any type of crime."

A recent police exercise codenamed Comcheck brought attention to large City financial institutions when it revealed major lapses in computer security.

A report on the exercise will show that some City organisations, including banks, cannot tell if hackers have broken into their computer systems.

The computer security checks are simply not in place to catch hackers.

"We've seen some incredible things in banks and finance houses," said Detective Inspector Norman Russell of the City of London Fraud Squad.

He said some firms had security systems in name only and paid lip-service to password security. Dealing rooms in particular are seen as an easy target. A recent survey of banks across Europe by the Computer Industry Research Unit (CIRU), a private company with government links, revealed that unprotected telephone lines were at major risk from hackers.

CIRU is compiling a database of hacking incidents in the City and it reports a rapid increase in the number of cases.

The irony, it seems, is that hackers know that the larger and more "successful" the crime, the less likely it is that a prosecution will follow. If they get caught before they get their hands on the cash they will probably end up in court, but if they hide their tracks and the losses are not discovered until much later, when the funds have been withdrawn, the chances of a prosecution being brought are diminished.

In some cases companies fearful of bad publicity allow the hackers to resign and take with them a good reference and a golden handshake.

■ *Lindsay Nicolle and Tony Collins are on the staff of "Computer Weekly".*