FEATURE

The Thin Blue Line

Two hackers sit conversing on a BBS, hundreds of miles apart. The only noise in the room is the hum of computer terminals and the incessant chattering of an outdated line printer. The screen of the terminal shows that they have just managed to gain access to a remote UNIX machine.

Without warning the door bursts inward, and in three simultaneous raids four men charge in, claiming to be police officers. Everything happens very quickly, and before the hackers have had a chance to think, they have been led away from the computer, caught red-handed. *New Scotland Yard's* latest raid has been a success.

Caught in the Act

The scene described above is accurate, if slightly misleading. Each 'hacker' arrested and charged was in fact involved in *Operation Skye*, the computer crime investigation course run by *New Scotland Yard's Computer Crime Unit* (*CCU*), at the *Police Staff Training College*, Bramshill. Over a four-week course, officers from many of the regional fraud squads pitted their wits against a problem which even the famous Sherlock Holmes could not have cast aside as elementary.

The Bramshill programme consists of two separate courses, tackling different aspects of the problem. During the first week, officers attending the course were instructed in how to obtain evidence from a DOS-based computer. Obviously, as computers become more commonplace, they will crop up as evidence with increasing regularity. As yet, most criminals still do not realise the evidential value of their own PCs. 'A lot of people still assume that, when you delete something, it is gone for ever,' commented Detective Sergeant Simon Janes, one of the officers responsible for running the course. 'However, you and I know that that is not the case.'

The second course lasts for three weeks, and tackles many of the different aspects of computer crime - hacking, viruses, unlawful access, telecommunications fraud etc. Although this course and others like it are designed for detectives from the regional Fraud Squads throughout England and Wales, the current course attendees ranged from far and wide, with one officer travelling from Hong Kong to attend.

Aims and Objectives

The objective of the course is very simple: that at least one member of each regional Police Service should be capable of taking on an investigation into possible offences under the UK *Computer Misuse Act* (*CMA*). 'As it stands at the moment, the *CCU* is the only dedicated unit in England - computer crime investigation at a local level is usually dealt with by the local Fraud Squads,' explained Janes.

Each police service can nominate whom they choose to send on the course. Nominees are usually taken from the ranks of Detective Constable, Sergeant or Inspector, but this is not a hard and fast rule. This present course even included a civilian, who was employed to assist the Police.

Janes makes a clear distinction between training detectives to be computer experts and training detectives in how to investigate typical computer crimes: 'We're not training detectives to be computer experts - we could never do that, and would not wish to. We aim to teach them how to manage an incident and how to investigate it. Obviously, part of that management issue is knowing when and where to go to get help.'

The question is very much one of knowing the procedures. Janes draws an analogy with the investigation of an assault. 'If a man is stabbed, he will be taken to hospital and seen by a surgeon. That surgeon would be able to supply further information, such as the size and type of the weapon used. In order to know that, you need to know a bit about what happens in a hospital. The officer investigating may not be an expert in knife wounds, but should know how to extract the necessary information from someone who is. It's a similar situation with computers.'

DI John Austen, the course organiser, agrees. 'We try to give them confidence in dealing with computer crimes that they would ordinarily have difficulty investigating. In that way, we can best serve the needs of the victim.'

Taught or Tort?

Lectures run parallel with the development of *Operation Skye*. These are aimed to tie in with what the 'hackers' are doing - for example, the lecture on *VMS* neatly coincides with the penetration of a large *VMS* installation.

The lectures are generally supplied by experts in their particular field. 'For example,' said Janes, 'yesterday Jim Bates was at Bramshill. He was here in two roles. Firstly, he gave a lecture about DOS viruses and how they worked. Secondly, one of the teams had reached a stage where they needed to know a lot more about viruses, so in the afternoon they sat down with Jim and questioned him.'

This mixture of the practical with the theoretical gives officers the benefits of both systems. The investigative side of the course is sufficiently realistic to be able to give a sense of the 'thrill of the chase', giving the often turgid theoretical aspects more immediacy. It also allows the students to put what they have learned to immediate practical use.

As the three weeks progress, the number of virus attacks and hacking offences increases. Each team receives more and more complaints, until they have gathered enough evidence

Detective Inspector John Austen plotting at the last Bramshill training course: 'You only learn when you make mistakes…' he commented wickedly.

to move in on the suspects. During the build-up to the arrest, as much realism as possible is brought into the scenario; officers even have to undergo a mock television interview in order to inform a 'concerned public' about the extent of the problem.

Misinformation

This gradual increase of pressure is masterminded by DI John Austen, leader of the *CCU*. Austen sits in the control room, surrounded by 'survivors' from previous years' courses. Together, they form a team which keeps the students busy with reports of new incidents. Various members of staff play the role of victims of the hackers, and officers get the chance to see first-hand how confusing such an investigation can become.

A lot of work goes into each part of the scenario. In the case of the virus outbreak, Austen's team has to work out how the virus was written, what it did, and how and where it spread. With this task accomplished, the next job is to give the course members just enough information to be able to work out what is going on. Balancing between making life too easy and too hard is difficult, and clues (and red herrings) are added as necessary. 'At the end of the day, we would like the students to be able to work out most or all of it,' said Janes, 'but they are going to have to work for it.'

Many of the features of the course are drawn from the personal experience Austen has gained through the *CCU*. 'You only learn when you make mistakes,' said Austen, 'and many of the exercises on the course are based on real incidents which have happened to me or my officers.'

'The thing to remember about the course is that there's nothing to pass at the end of the day. There's no examination, and candidates aren't failed. It is all about learning. The students get out of it as much as they put into it,' explained Austen.

Hot on their Heels

The proof of the pudding is very much in the eating: Austen has set up an ambitious course which attempts to cover a lot of ground in a comparatively short time. Do the students feel that their three weeks of hard slog is of any value when they return to their units?

Casting around for opinion, the general feedback on this occasion was very positive. Mark Morris (the latest addition to the *CCU*), seemed pleased with what he had learned. 'We're into the third week of the course now. It is certainly stressful, but overall, I think it has been very useful. The thematic way in which the lectures tie in with what's happening in the investigation is good, and you really find yourself getting into the scenario. I've learnt a huge amount on this course - I think everybody has.'

Several of the officers helping to run the course had also attended previously as students. Rupert Groves, from the Bedfordshire Police Force, completed the course five years ago, and found the experience invaluable. 'At the time I came on the course, I was completely computer illiterate, and found it extremely difficult. Before the course, if I had been called in to take a complaint from someone about a computer crime, I would have been floundering. Since attending the course, I have been involved in a number of *CMA* cases which have been successful. What the course did for me was give me the confidence to approach victims of, and experts on, computer crime, and understand what was happening and what needed to be done.'

Crime and Punishment

Austen is confident that the Bramshill course makes the police forces of the United Kingdom better equipped to deal with computer crime. The police are making an effort to tackle the problem - is there anything which can be done to help them? 'The computer industry has always given us tremendous support. When we've asked for anything, it has never been refused. The problem is that the public often don't recognise computer crime. They may get violations of their system, or observe unexplained occurrences, but they don't realise that they have actually been the target of criminal activity.'

The problem of not submitting a complaint is compounded by the question of whom to complain to. 'Users also don't know where to go to explain it to the police. If you were to walk into your local police station and speak to the uniformed desk sergeant, they probably wouldn't understand what you were talking about. What I would say is that anyone who has suffered a computer crime can contact us at *Scotland Yard*, or any of the Fraud Squads around the country, and there will always be an officer to deal with them.'

Happy Conclusion

The idea of gaining confidence was mentioned several times by the students, and the results are almost certainly worth the effort. Seven days after this interview was taken, the officers involved in *Operation Skye* successfully caught their targets red-handed. Hackers had better lie low for some time - contrary to popular computer underground opinion, the police can and will pursue computer criminals.